CHAPTER 4 — MANAGEMENT INFORMATION SYSTEMS

ARTICLE 1 — ELECTRONIC DATA PROCESSING

Revised October 17, 1994

41010.1 Policy

The Director and Executive Management of the Department recognize Information Technology as an indispensable tool of modern government. Therefore, it is the policy of the Director to support and promote the departmental use of innovative information technologies in order to increase worker productivity, improve departmental services, and strengthen the overall effectiveness of management, while saving money and thus reducing the overall cost of government.

41010.2 Purpose

The purpose of the Department's EDP policy is to ensure that proven management methods for the guidance and control of planning, acquisition, development, operation, maintenance, and evaluation of information management applications are established in a manner that provides for the most efficient, effective, and economical use of the Department's resources for information technology. This policy also establishes clear lines of authority and responsibility for information management within the Department. Consistent with this policy, the primary purpose of CDC computer-based ITS is to assist in overall management of the day-to-day operations of CDC's headquarters, facilities, and parole offices.

41010.3 Definitions

Acceptance Testing

Testing which ensures that a computer system meets the needs of the organization and the end-user.

Access

To gain entry into, or to instruct or communicate with, the logical, arithmetical, or memory function resources of a computer, computer system, or computer network.

Access Authorization

The granting of permission to execute a set of operations in a computer system.

Access Control

Tasks performed by hardware, software, and administrative controls to monitor a computer system's operation, ensure data integrity, perform user identification, record system access and changes, and grant access to users.

Accountability

The ability to trace violations or attempted violations of system security to the individual(s) responsible.

Application Disaster Recovery Plan

A plan devised to process a computer application (application) after it has been disrupted for some period of time.

Audit Requirements

A section of the EDP audit reviews ITS documentation; each system not exempt from the audit requirements shall have an approved risk analysis report.

Authentication

The procedure for identifying or verifying the eligibility of a station, originator, or individual to access specific categories of information.

Authorization

The power granted by management to specified individuals allowing them to approve transactions, procedures, or total systems.

Back-up Procedures

Methods used to duplicate computer programs and files prior to any loss or damage to such information, and the methods to recover such information after a disaster or system failure.

Baseline Security Controls

A set of general controls designed to meet an acknowledged level of security control that should be in place within all properly run computer centers.

Bulletin Board System

An electronic message system which runs generally on microcomputers and allows users to enter and read information.

Call Back

A method used to identify a terminal that is dialing into a computer system, whereby the system disconnects the calling terminal and then reestablishes the connection by dialing the telephone number of the calling terminal.

Classification

The assignment of information, including a document, to a category on the basis of its sensitivity concerning disclosure, modification, or destruction.

Client (User)

The individual or organization that utilizes a product.

Computer Contaminant

Any set of computer instructions that, outside the intent and without the permission of the owner of such information, is designed to modify, damage, or destroy a computer, computer system, or computer network, or to record or transmit information within a computer, computer system, or computer network. Such contaminants include, but are not limited to, the group of self-replicating or self-propagating computer instructions commonly termed viruses, trojans, or worms which are designed to affect computer programs or data, consume computer resources, modify, destroy, record or transmit data, or otherwise usurp the normal operation of the computer, computer system, or computer network.

Computer Network

Any system that provides communication among one or more computer systems and input/output devices including, but not limited to, display terminals and printers connected by telecommunication facilities.

Computer Program or Software

A set of instructions, or statements and related data, which when executed in actual or modified form cause a computer, computer system, or computer network to perform specified functions.

Computer Security

The technological safeguards and managerial procedures which can be applied to computer hardware, programs, data, and facilities to ensure the availability, integrity, and confidentiality of computer-based resources. This can also include assurance that intended functions are performed as planned.

Computer Services

Includes, but is not limited to, computer time, EDP or storage functions, or other uses of a computer, computer system, or computer network.

Computer System

A device or collection of devices, including support devices but excluding calculators that are not programmable and not capable of being used in conjunction with external files, one or more of which contain computer programs, electronic instructions, input data, and output data, and which performs functions including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control.

Confidential Information

Information maintained by State agencies that is exempt from disclosure under provisions of the California Public Records Act (GC 6250-6265 or other applicable State or federal laws). See SAM 4841.3.

Contingency Planning

The procedure for developing a back-up plan to restore business and data center operations in the event of a disaster or interruption; also termed disaster recovery planning or business resumption planning.

Contingency Program

The everyday work activities and procedures that fulfill the requirements of recoverability (e.g., backing-up critical data files).

Continuing Costs

Costs associated with the operation and maintenance of an information technology system or application that are realized after development and implementation of the system. See SAM Section 4819.2

Correctness

1) The extent to which software conforms to its specifications and standards; and, 2) (a) the extent to which software is free from design and coding defects (i.e., "fault-free"), (b) the extent to which software meets user expectations.

Cost of Quality

The cost of quality for a product is the sum of prevention, detection, correction and client costs. Prevention cost is the total cost incurred during product development and prior to general release. Detection, correction, and client costs are post-release costs associated with reworking due to defects. QA shall be considered cost-effective when post-release costs are reduced by an amount greater than any increase in prevention costs resulting from the inclusion of QA in the development process.

Cost Thresholds

Cost thresholds are assigned to agencies based on their size and past experiences with information technology projects. CDC is a Category1agency. Therefore, any CDC project exceeding $500,000 in cost is a reportable project.

Critical Application

An application so important to the Department that its loss or unavailability is unacceptable. With a critical application, even short-term unavailability of the information provided by the application would have a significant negative impact on the health and safety of the public or Department employees, the fiscal or legal integrity of departmental operations, or the continuation of essential programs.

Critical Functions, Systems, and Resources

Elements vital to the organization's operation and possibly the organization's survival.

Current Risk

Current risks are evident and continuing, and are inherent in a business operation, location, or process.

Custodian of Information

An employee or organizational unit (such as a data center or information processing facility) acting as caretaker of an automated file or database.

Data

A representation of information, knowledge, facts, concepts, computer software, computer programs, or instructions. Data may be in any form, such as in storage media, stored in the memory of the computer, in transit, or as presented on a display device.

Data Base Integrity

The accuracy, completeness, and timeliness of information contained in a database.

Data Integrity

The state that exists when computerized data are the same as in source documents and have not been exposed to accidental or malicious alteration or destruction.

EDP

The execution of a programmed sequence of operations upon data.

EDP System

Collection of methods, procedures, and resources designed to accept input, process data, deliver information, and maintain files to provide direct support of an organization's basic transactions and operations.

Data Protection

Measures to safeguard against occurrences that could lead to the modification, destruction, or disclosure of data.

Data Security

Protecting data from modification, destruction, or disclosure.

Data Transmission

The sending of data from one part of a system to another.

Data/Information Storing

The preservation of data in various data media for direct use by the system.

Defect

A variance from specifications/standards or an attribute/function not contained in the software requirements specifications.

Defect-Prone Process

A process/activity during which a high number of defects occur.

Desk Checking

An informal evaluation technique in which the person who developed a unit of code inspects it visually to identify possible errors or violations of development standards.

Development

Activities or costs associated with the analysis, design, programming, staff training, data conversion, acquisition, and implementation of new information technology applications. See SAM Section 4819.2.

Disaster

An occurrence causing destruction and distress, after which a business is deemed unable to function.

Disaster Recovery Operation

The act of recovering from the effects of disruption to a computer facility, and the preplanned restoration of facility capabilities.

Disaster Recovery Plan

The preplanned steps that make possible the recovery of a business computer facility or the applications processed therein. Also called a contingency plan or business resumption plan.

EDP Equipment

EDP equipment is defined in SAM Section 4819.2 as follows:

- Central processing units and all related features and peripheral units, including processor storage, console devices, channel devices, etc.
- Communications devices used for the transmission of data, such as modems, data sets, multiplexors, concentrators, switches, local area networks, private branch exchanges, network control equipment, and microwave or satellite communications systems.
- Input-output (peripheral) units (off-line or on-line) including: terminals, card readers, optical character readers, magnetic tape units, mass storage devices, card punches, printers, computer output to microfilm converters, video display units, data entry devices, FAXs, teleprinters, plotters, optical sense scanners, or any device used as a terminal to a computer and control units for these devices.
- Minicomputers, microcomputers, personal computers, and all peripheral units associated with such computers.
- Special purpose systems including word processing, magnetic ink character recognition, optical character recognition, photocomposition, typesetting, and electronic bookkeeping.

EDP Personnel

All State personnel employed in EDP classifications, as defined by the DPA or the Trustees of the California State University and Colleges, and all personnel of other classifications in State EDP organizations who perform technology activities for at least 50 percent of their time. Users of personal computers and office automation are not included in this category unless they are employed in EDP classifications or spend at least 50 percent of their time performing information technology activities. See SAM Section 4819.2.

EDP Project

A project that encompasses computerized and auxiliary automated information handling including systems design and analysis, data conversion, computer programming, information storage and retrieval, data transmission, requisite system controls, simulation, and related interactions between people and machines; synonymous with Information Technology Project. See SAM Section 4819.2.

EDP Supplies

All consumable items and necessities (excluding equipment defined as EDP equipment) to support information technology activities and EDP personnel, including:

- Documents (such as standards and procedures manuals, vendor-supplied systems documentation, and educational or training manuals).
- Equipment supplies (such as printer forms, punch card stock, disk packs, "floppy" disks, magnetic tape, and printer ribbons or cartridges).
- Furniture (such as terminal tables and printer stands). See SAM Section 4819.2.

Emergency Response

The immediate action taken to protect hardware and sensitive magnetic media in the event of natural disasters, fire, power failures, equipment breakdown, theft, vandalism, or tampering.

Failure

Inability of a product or service to perform its required functions within previously established limits.

Hardware

The physical equipment or machinery (computers, terminals, printers, disc drives, etc.) used in EDP.

Information Assets

All categories of automated information including, but not limited to, records, files, data bases, and information technology facilities, as well as equipment and software owned or leased by the Department.

Information Integrity

The condition in which information or programs are preserved for their intended purpose, including the accuracy and completeness of ITS and data maintenance within those systems.

Information Processing

The systematic performance of operations upon data such as handling, merging, sorting, and computing; synonymous with EDP.

Information Security

The protection of automated information against unauthorized access (accidental or intentional), modification, destruction, or disclosure.

Information Technology

All computerized and auxiliary automated information handling, including: Systems design and analysis; conversion of data; computer programming; information storage and retrieval; voice, video, and data communications; requisite system controls; simulation; and, all related interactions between people and machines. See GC Section 11702(a).

Information Technology Procurement

See DOM 45000.

Information Technology Project

See EDP Project.

Injury

Any alteration, deletion, damage, or destruction of a computer system, computer network, computer program, or data caused by access.

Input-Output Unit/Device

The equipment used to communicate with a computer; commonly termed I/O (Input/Output).

Integration Testing

Testing performed on groups of modules to ensure that data and control are passed properly among modules.

Life Cycle

The anticipated length of time that the information technology system or application can be expected to be efficient and cost-effective and can continue to meet the agency's programmatic requirements; synonymous with operational life of a system. See SAM Section 4819.2.

Load Management

The objective of load management is to meet user commitments while allocating resources to allow their maximum utilization at the lowest possible cost; additionally, to provide reports to management on current and projected processing loads for short- and long-term capacity planning.

Long-Term Capacity Planning

The objective of long-term capacity planning is to develop methods and means for ensuring that hardware, system software, communications, and system design meet the long-term objectives for additional processing required by new applications, integration of new processors and platforms, and new generations of software. This plan encompasses a five- to seven-year period and is designed to help determine budget requirements and goals for the Department.

Maintenance

The ongoing process by which functional elements of hardware and software are corrected and enhanced to accommodate changes in organizational needs.

One-Time Costs

Costs associated with the analysis, design, programming, staff training, data conversion, acquisition, and implementation of new information technology applications. See SAM Section 4819.2.

Operational Life

See Life Cycle.

Operations

Activities or costs associated with the continued use of information technology applications. Operations includes personnel associated with computer operations, including network operations, job control, scheduling, and key entry. It also includes the costs of computer time and other resources needed for processing. See SAM Section 4819.2.

Owner of Information

An individual in a particular position or an organizational unit having responsibility for making classification and control decisions regarding an automated file or data base.

Peripheral Unit/Device

A device which may be connected to a computer's central processor.

Physical Security

The protection of information processing equipment against damage, destruction, or theft, of information processing facilities against damage, destruction, or unauthorized entry, and of personnel from potentially harmful situations.

Post Implementation Evaluation Report

The review of a computer, computer system, or computer network that has been in operation for at least six months and no longer than two years for the purpose of matching the requirements of the system against what has been produced so as to ensure that stated requirements have been met.

Potential Risk

Risk outside normal and purposeful business operations resulting from some indeterminate action whether intentional or unintentional.

Previously Approved Effort/Project

An information technology activity or project approved previously by the Office of Information Technology (OIT) or the agency's executive officer in accordance with SAM Section 4819.3. Completion of an approved FSR and an approved Post-Implementation Evaluation Report are required in order to qualify an activity as a previously approved effort. Eligible activities include converting software, meeting modified needs, improving the effectiveness of the activity, program or system maintenance, and the extension of existing services to new or additional users performing essentially the same functions as those the project was originally designed to support. A previously approved effort/project must use substantially the same equipment, facilities, technical personnel, supplies, and software to meet the same requirements or to meet normal workload increases. ("substantially the same equipment" does not include the addition, upgrade, or replacement of a central processing unit.) See SAM 4819.2.

Privacy

The right of individuals and organizations to control the collection, storage, and dissemination of information about themselves.

Problem Reporting/Tracking

A process of reporting outstanding problems, assigning them for resolution, and closing them out when the user has been notified that the problems have been solved.

Process

The work activities that produce products, including the efforts of people and equipment.

Product

The output of a process, including the goods and services produced by individuals and the organization.

Program

The set of instructions by which a computer operates to accomplish a specific task.

Program Application Manager

Department supervisory and management staff responsible for managing or supervising employees' use of an automated file or database.

Programming

Detailed design encompassing the actual development and writing of program units or modules.

Project

A planned sequence of tasks to respond to a problem or opportunity; an activity with a beginning and an end and containing a set of resources.

Proprietary Software

Software packages which are developed by independent vendors and marketed to users.

Public Information

Any information prepared, owned, used, or retained by a State agency and not exempted specifically from disclosure requirements under the PRA (GC 6250-6265) or other applicable State and federal laws.

Quality

The extent to which a product meets the expectations and requirements of the user.

QA

(1) A staff function designed to support line management in performing the QC function. As such, QA identifies the processes (both good and bad) which affect quality, and is used to advise management of such effects. A management decision may then be necessary to ensure that QC techniques are implemented and maintained; and,

(2) The function that uses measurement and analysis to continually improve processing, procedures, and standards so that management can be reasonably assured of their staff following such methods, procedures, and standards, as well as staff's ability to produce products which meet specified requirements.

QC

(1) The collection of activities to ensure that defects are neither made nor implemented. While QA monitors the processes involved in the production cycle, QC is an integral part of work and is the responsibility of each employee; and,

(2) A line function used to measure quality associated with specific products or services. QC is the responsibility of each ITS area, and it is the function responsible for the quality of the work being done within a specific area or for a specific project.

Quality Improvement Program

A program designed to reduce the number of defects produced.

Regression Testing

Testing which is applied after changes have been made to ensure that no unwanted changes have been introduced.

Reportable Project

A planned development activity or planned acquisition of new or enhanced information technology capabilities (as defined in SAM Section 4819.2) meeting one or more of the following criteria:

- The project involves total estimated development or acquisition costs greater than the cost threshold established for the agency (see SAM Section 4902.12 for a definition of "cost threshold").
- The project involves a budget augmentation for an increase in the agency's existing information technology activities, to be obtained through submission of a BCP or a Budget Revision.
- The project is a new system development or acquisition made in response to a legislative mandate, or the project is subject to special legislative review as specified in budget control language or other legislation.
- The project involves direct public access by private sector organizations or individuals to State data bases.
- The project involves contracts for professional, managerial, or technical services (excluding services received through interagency agreements) exceeding a total of $25,000.
- The project involves the acquisition of any microcomputer commodities and the agency does not have an approved Workgroup Computing Policy. See SAM Sections 4989 et seq.
- The project involves acquisition, upgrade, or installation of a mainframe or mid-range, multi-user central processing unit.
- The project involves installation or expansion of wide area network data communication services other than those offered by the DGS, Division of Telecommunications, or a State consolidated data center as defined in SAM Section 4982.
- The project involves one or more of the following emerging technologies and more than $25,000 will be spent on acquisition of hardware or software required for the technology:
  - Document imaging.
  - Geographic information systems.
  - Computer aided systems engineering.
  - Expert systems/artificial intelligence.

Requirement

The specification(s) for satisfying a user need is associated with a standard by which the satisfaction of that need can be measured.

Resource Management

The determination of current and short-term needs for hardware, system performance, communication, and the allocation of such resources to meet the overall goals and current short-term plans of the Department. Resource Management requires the gathering of data about new processing needs and applications not addressed in long-range planning as well as any other information which impacts current system resources.

Risk

A measure of the relative value attached to certain circumstances and conditions inherent in any business operation or change to such operation; the likelihood or probability that a loss of information assets or a breach of security may occur. Risks are either current or potential.

Risk Analysis Content:

Technical Analysis

For each risk scenario, specification of the threat and identification of the potential safeguards/controls involved. Each control should be discussed along with its intended purpose and the types of threats against which it is effective. If no safeguards are found, a statement to that effect shall be provided.

Operational Analysis

Each control identified during technical analyses should be analyzed and its impact on current operations should be discussed. All operational constraints which would make the safeguard difficult or impractical to implement or operate should be discussed. Risks to be accepted given the operational unacceptability of their safeguards shall be identified here.

Economic Analysis

Discusses the cost benefit for all controls which are technically and operationally feasible.

Risk Acceptance Summary

Lists all risks whether acceptable or unacceptable. If acceptable, indicates the basis for acceptance.

Risk Controls Summary

Presents the controls to be used for eliminating or reducing risks identified in the risk acceptance summary. Each control should be described, as well as the loss reduction or effect and the primary and secondary threat categories against which the control is effective.

Countermeasures

Any type of procedure, (e.g., physical, procedural, hardware, software, personnel) used to counteract a threat to the system.

Risk Analysis Management Report:

Summary

A concise overview of the risk analysis, beginning with a statement describing the scope and objectives of the study and followed by the recommendations for risk acceptance and alternatives for reducing or eliminating the unacceptable risks.

Scenario Summary

A summary of the essential data from the risk analysis.

Risk Management

The process of taking actions to avoid risk or reduce risk to acceptable levels.

Risk Management Process

Risk management performed by a manager to identify the risk, assess the level of risk, and by analytical process create a plan for the acceptance, rejection, or control of the risk. This work is carried out by application of a well defined process called risk analysis and culminates in a Risk Analysis Report and Risk Reduction Decision Study.

Risk Analysis

Involves identifying the availability of potential safeguards, determining the operational and economic feasibility of such safeguards, and developing a Risk Reduction Decision Study for presentation to management (this process corresponds to the identification of alternatives, cost-benefit analysis, selection of the best alternative, and conceptual system design phases of a generic systems approach).

Risk Reduction Analysis

Involves identifying the assets and resources that are at risk, the threats to those assets and resources, the vulnerabilities in the risk environment which might allow the threats to materialize, the estimated frequency with which the threats might occur, the safeguards currently in place, and the cost/impact that could be incurred if the threats to the risk environment were to materialize (this process corresponds to the problem definition and analysis of the "current problem" steps in a generic systems approach).

Management Decision

Management decides which risks are acceptable. For those risks not currently acceptable, management decides which of the alternatives shall be implemented and approves the resources required to purchase, design, develop, and implement them (this process corresponds to the management decision phase of a generic systems approach).

Development of Risk Reduction Plans

Outlining of the tasks to be performed to implement the safeguards selected by management. Tasks include: identification of the specific safeguards; assignment of responsibility, design and development, or purchase; and, implementation of the safeguards. Plans should also include a timetable of milestones leading to implementation (this process corresponds to the detailed design and development/testing phases of a generic systems approach).

Implementation and Maintenance of Safeguards

Involves the installation, operation, and maintenance of new or modified safeguards. Implementation includes personnel training and coordination of any changes in operations with affected personnel.

Sensitive Information

Information maintained by State agencies which requires special precautions to protect it from unauthorized modification or deletion (see SAM Section 4841.3). Sensitive information may be either public or confidential (as defined above).

Software

Computer programs, procedures, rules and any associated documentation or data pertaining to the operation of a computer system.

Supporting Documentation

Information pertaining to the design, construction, classification, implementation, use, or modification of a computer, computer system, computer network, computer program, or computer software.

System Testing

A generic term that differentiates various types of higher order testing from unit testing.

Total Quality Management

Consists of continuous process improvement activities involving everyone in an organization--managers and workers--in a totally integrated effort toward improving performance at every level. This improved performance is directed toward satisfying such cross-functional goals as quality, cost, schedule, mission need, and suitability. Total Quality Management integrates fundamental management techniques, existing improvement efforts, and technical tools under a disciplined approach focused on continuous process improvement. The activities are focused ultimately on increased client/user satisfaction.

Unit Testing

Testing performed on a single, stand-alone module or unit of code.

User of Information

An individual having specific limited authority from the owner or program application manager of information to view, change, add to, disseminate, or delete such information.

Validation

The process of comparing a product in any stage of its development with specified requirements to determine whether the correct product is being produced.

Victim Expenditure

Any expenditure reasonably and necessarily incurred by the owner or lessee to verify whether a computer system, computer network, data, or computer program was altered, deleted, damaged, or destroyed by the access.

Vulnerability

Susceptibility of a system to a specific threat, attack, or harmful event, or the opportunity available for a threat agent to mount that attack.

Vulnerability Assessment

A review of a computer system or program to determine its susceptibility to loss or unauthorized use.

Walk-Through

A review process in which a designer or programmer leads one or more members of the development team through a segment of documentation or code that he or she has written, and other team members ask questions and make comments about technique, style, possible errors, violation of development standards, and other issues.

41010.4 Revisions

The Assistant Director, OOC, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

41010.5 References

GC §§ 6250 - 6265, and 11702 (a).

SAM §§ 4819.2, 4819.3, 4819.12, 4841.3, and 4849, et seq.

DOM § 45000.

ARTICLE 2 — EDP RESPONSIBILITY

Effective December 22, 1992

41020.1 Policy

The Department's executive management is responsible for the establishment of departmental policy pertaining to the use of information technology, the prioritization of departmental resources, and strategic planning and leadership to seek out opportunities for employing information technology toward achievement of the Department's mission, goals, and objectives. Department executive leadership is responsible for ensuring that information technology is used within the guidelines contained in this manual section and those established by other control agencies.

41020.2 Purpose

The purpose of this policy is to ensure that departmental resources and information technology are used optimally in achieving the Department's mission, goals, and objectives. Additionally, this policy assures that uses of information technology follow the guidelines established internally by CDC management and externally by State control agencies.

41020.3 Management Information Systems Committee

Revised October 6, 1993

The MIS Committee shall:

- Provide executive leadership in the development of EDP projects and policy.
- Enforce compliance of the project approval process with the Department's Strategic Plan.
- Prioritize EDP projects in terms of their importance to the Department's Strategic Plan.
- Review and enforce policy and procedures in support of EDP projects.
- As individual committee members, serve as liaisons with their respective end user communities to promote, coordinate, and facilitate automation efforts, and to ensure effective communication regarding EDP-related issues throughout all levels of the Department.
- Educate management in the advantages of automation, new EDP-related technical innovations, and methods to maximize the efficiency and benefits of automation, and to minimize EDP development and operating costs.
- Provide review and approval of all information technology procurements not covered under the approved Workgroup Computing Policy.
- Provide ongoing review of CDC-approved EDP projects, terminating those projects which are no longer consistent with the Department's Strategic Plan.

Note that the MIS Committee does not make any decisions on funding of ITS projects. The committee only recommends the prioritization of these projects.

See DOM 43020.4, Information Management Annual Plan, for additional information about the role and responsibilities of the MIS Committee.

41020.3.1 MIS Committee Composition

The MIS Committee is comprised of the following voting staff:

- The Chief Deputy Director (Chairperson).
- Three representatives from ASD.
- Three representatives from EC&ISD.
- Five representatives from Institutions Division.
- Three representatives from P&CSD.
- One representative from P&CD.
- One representative from PIA.

These representatives shall be appointed for an indeterminate period.

In the absence of the Chief Deputy Director, the Deputy Director of ASD shall chair MIS Committee meetings.

The committee shall meet on a quarterly basis and more often as needed. MIS Committee meetings are generally open to all wishing to attend.

41020.4 Responsibility MIS-SU

Revised October 6, 1993

MIS-SU provides functional support to the MIS Committee. The MIS-SU's responsibilities include: (1) coordinating MIS Committee meeting agendas; (2) coordinating the review of proposed ITS and to furnish recommendations for MIS Committee review; (3) preparing annual updates for the Cabinet on all CDC automation efforts for the current year and on strategic planning for the coming year; (4) developing, coordinating, and participating in presentations for the committee that address current technical innovations; (5) coordinating the review of ITS concepts to ensure compliance and consonance with the budget cycle; (6) recording the actions and decisions of the MIS Committee for distribution to

appropriate departmental staff; and, (7) conducting special projects as assigned by the committee.

Departmental Workgroup Computing Coordinator

The Workgroup Computing Coordinator's responsibilities include: (1)ensuring that workgroup computing hardware and software requests comply with departmental and control agency policy requirements; (2)preparing the appropriate certification documents for workgroup computing procurements; (3) providing assistance in the completion of workgroup computing requests; (4) maintaining the departmental Workgroup Computing Policy and Modem Policy, as well as related equipment request forms for distribution to departmental staff; (5) overseeing the personal computer Post Implementation Evaluation Report (PIER) process; (6) maintaining the departmental personal computer equipment inventory; and (7) maintaining a record of all personal computer procurements, including those justified through the use of an FSR, a CDC Internal Summary Fact Sheet, or the approved Workgroup Computing Policy.

Department Information Security Officer

The CDC Information Security Officer (ISO) is assigned management responsibility for overseeing and administering the Centralized Information Security Program and is charged with the responsibility of assuring the Department's compliance with the SAM 4840, Security and Risk Management; 4989.7, Security of Personal Computer Systems; and 20013, EDP Audit Requirements. This program encompasses all automated ITS for which CDC has administrative responsibility. It includes the procedures, guidelines, and safeguards that are required to protect data, confidentiality, and privacy rights and ensures the integrity, audibility, and controllability of these ITS. All new policies and revisions of existing policy relating to automated information security will emanate from this office.

ISD

It is the responsibility of ISD to establish and maintain the departmental EDP strategic planning process and to oversee the development of all departmental EDP policies, including assurance that such policies meet control agency guidelines. ISD is also responsible for ensuring that such considerations as compatibility and connectivity of all proposed automated projects are taken into consideration in the project approval process.

ISD is responsible for the development, maintenance, operation, and support of all departmental PC applications except Institutions Division projects, and for all automated systems requiring control agency oversight unless specifically delegated to another unit by the MIS Committee.

Under the User Project Management concept, the User Manager is responsible for all project reporting to control agencies, the user division, and the MIS Committee. ISD provides technical management and staff who work as team members accountable to the User Manager on the project and to ISD on technical issues (e.g., project schedules).

ISD is also responsible for tracking all projects approved by the MIS Committee, and ensuring that all projects comply with State reporting requirements. All project reporting to control agencies shall be coordinated through ISD, which shall maintain correspondence files on control agency reporting.

ISD shall report directly to the appropriate Division (User Manager Concept) associated with each EDP Project, and to the MIS Committee on all approved projects.

ISD is responsible for the security of information technology facilities, and for software and equipment used in automated information processing at all sites under ISD custodial responsibility. ISD also maintains the CDC Operational Recovery Plan for these systems.

ISD provides functional support and assistance on all facility automated systems (except personal computers) to facility AISAs.

ISD is also responsible for ensuring compliance with State audit requirements relating to the integrity of information assets. This includes systems auditing under ISD's custodial realm of responsibility through participation in the departmental Peer, and PFAB's auditing processes.

ISD is responsible for establishment of the Department's overall automation infrastructure and the successful use of automation within the Department.

ISD consists of five major areas: Application Development and Maintenance Section, Technology Support Section, Project Initiation Unit, CMIS Section, and the Data Center Section.

Technology Support Section

The Technology Support Section provides support services to ISD in the following areas: personnel, recruitment, staff training, budgeting, procurement, interagency agreements and contract management, quality programs, space planning, and general office support. This section also provides support services to all branches of the EC&ISD for personnel, recruitment, and training.

Project Initiation Unit

The role of the Project Initiation Unit (PIU) is to provide guidance and assistance to CDC staff in starting new information technology projects. This includes providing guidance in the development of project concept proposals, feasibility studies, and other documentation required to obtain approval of an information system project. The PIU is responsible for tracking all approved projects and ensuring that all projects comply with State reporting requirements. Functional support, assistance and direction is provided to the ISAs on all system related issues by the Applications Systems Section.

Data Center Section

The Data Center manages maintenance and support functions with the best available tools in order to increase the time that ITS are available to the users/owners. This section of ISD is responsible for the continuous operation and reliability of computer hardware, database systems software, the systems' databases, and communications networks, as well as the security of departmental ITS. As part of the Data Center, the Network Services Unit and the Hardware/Telecommunications Unit provide data communications services and support to ISD and to other functional units as needed, ensure that standard approved practices are adhered to within the Department, and provide and promote the use of consulting resources to the Department when developing new systems or planning changes to existing data facilities.

CMIS Section

The role of the CMIS Section is to develop a single automated offender information system which satisfies the needs of all users of CDC's offender information and serves as the hardware/software platform for all future systems development for the Department. Using state-of-the-art analysis techniques and project management tools, the CMIS Section is committed to providing the Department with an offender information system that meets the needs of the user community.

OISB

OISB has been designated the Department's primary provider of summary statistical information about inmates and parolees. The OISB responds to special information requests, compiles statistical reports, and prepares legislative estimates and population projections. The OISB is responsible also for coordinating the timely, accurate, and consistent coding and entry of data, and performs data integrity QC functions for OBIS and for classification, incident, and other major computerized inmate and parolee databases.

Estimates and Statistical Analysis Section

The Estimates and Statistical Analysis Section is the primary source of summary statistical information on inmates and parolees under the jurisdiction of the Department. This section ensures that the Department has accurate data upon which to base program planning and direction. It also compiles and analyzes information for special projects, court cases, special task forces or programs, and prepares periodic statistical reports about inmates and parolees used in budget planning, legislative responses, and audits. The section prepares all departmental projections of future facility and parole populations, including inmate classification levels, and all population estimates of the impact of proposed legislation, ballot initiatives, and administrative policy changes. It also reviews such information to be disseminated by other branches and divisions outside of the Department.

TSS

TSS coordinates the timely, accurate, and consistent coding and entry of data, and performs data integrity QC functions for major computerized inmate and parolee ITS.

This section provides support to the MIS Committee to facilitate the development and automation of ITS, and conducts regular audits in the field and in Headquarters to maintain the accuracy and integrity of data. The section also provides necessary training for facility and parole region OBIS operators.

Business and Contract Services

BSS

BSS is responsible for the preparation of purchase documents for all EDP equipment and data-related items that are obtained through Headquarters.

BSS shall ensure that all requests submitted for purchase are complete and that the necessary documentation, such as certifications or FSRs, is included.

BSS is the departmental contact with the DGS, Office of Procurement, for all EDP procurement.

Contract Services

The Department's Contract Services Section shall supervise contracts entered into by the Department in a manner which:

- Conserves the financial interests of the State.
- Prevents, so far as possible, any thriftless acts by employees of the Department.
- Avoids thriftless expenditures.

The Contract Services Section assists departmental staff in the development of EDP contract requests, bids, and contracts to achieve program objectives within the legal and regulatory constraints of the State, and to ensure compliance with all departmental policies and procedures.

Warden/Regional Administrators

Each Warden and RPA is ultimately responsible for the security and utilization of all automated systems and data bases in the respective facility or region. This includes the integrity and accuracy of data entered and the physical security of the data, hardware, and the system itself.

Facility/Parole AISA/ Regional AISA

Under the direction of the Warden or designee, or Regional Administrator or designee, the facility or region AISA is responsible for the coordination of automated systems issues for the facility. This position acts as the primary contact for Headquarters on automation-related issues, including PC, the DDPS, and all other automated system concerns.

This position is responsible for coordination of staff training on PC applications and systems, justification and acquisition of PC equipment through use of PC, policy, local automated system application support, inmate access to computers, on-site user assistance, information system security, and QC oversight and audit coordination for all databases located in the area of assignment.

Facility/Regional Information Security Coordinators

Facility/regional Information Security Coordinators (ISC), in accordance with State and departmental security policies, are responsible to the Warden/RPA for overseeing policy and procedures on information security access at each facility.

The ISC shall work in coordination with the ISAs and the Department's Information Security Officer.

Departmental Managers/Supervisors

All managers and supervisors assigned supervision of a function automated by DDPS are responsible for:

- Preserving the security and integrity of the Department's information assets and managing the associated risks.
- Ongoing auditing to verify the accuracy and integrity of the data entered by subordinate staff.
- Ensuring that program staff and other users of the DDPS information are aware of and comply with information security policy and procedures.

End Users of EDP

Users are ultimately responsible for:

- The accuracy and integrity of the data they enter into any departmental application.
- Complying with all applicable laws, regulations, and administrative policies, as well as with any additional security policies and procedures established by the Department.
- Notifying their manager/supervisor of any actual or attempted violations of security policies, practices, or procedures.

41020.5 Revisions

The Chief, ISD, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

41020.6 References

DOM §§ 43030 and 43020.4.

ARTICLE 3 — ORGANIZATIONAL STAFFING AND TRAINING

Revised October 17, 1994

41030.1 Policy

It is the policy of the Department to create an automation organizational structure that is conducive to the successful implementation, maintenance, and control of the EDP environment. CDC shall create an EDP environment that ensures the appropriate use of all positions with EDP classifications and provides opportunities and career enhancement capabilities to all EDP employees.

41030.2 Purpose

The purpose of this policy is to ensure the creation of an EDP infrastructure that meets the needs of the Department. This policy fixes responsibility and authority for the creation of this process.

41030.3 Responsibility

The ultimate responsibility for creation of an automation organizational structure rests with the Director and Chief Deputy Directors of the Department, with functional responsibilities placed with the Chief, ISD. It is the responsibility of the Chief, ISD, to:

- Ensure that a training environment exists which meets State requirements for EDP-related classes of employees.
- Establish and coordinate the departmental testing process for EDP related classifications.
- Oversee the departmental EDP organizational structure.
- Provide input into the use of, and changes to, all departmental EDP positions.

41030.4 Training Policy

It is the policy of CDC to provide training to all EDP staff and the user community utilizing EDP equipment and software in order to ensure staff's overall effectiveness, success, and efficiency in providing automated solutions to departmental business problems.

41030.5 Training Purpose

The purpose of this policy is to provide training guidelines and assign appropriate departmental management responsibilities to ensure that all EDP staff, as well as the user community utilizing EDP equipment and software, are provided with the training necessary to perform their duties.

41030.6 Training Responsibility

It is the responsibility of the Chief, ISD, to establish and chair a departmental EDP Training Committee, with membership from each division as listed below. This committee shall be charged with identifying training needs for all EDP staff and the end user community and shall meet quarterly. The committee shall be comprised of representatives from:

- ISD (Chief).
- MIS-SU.
- P&CSD.
- TSB (representing all other departmental interests).

The EDP Training Committee shall be responsible also for establishing EDP training standards for all Department end users utilizing EDP equipment or software. Training plans approved by this committee shall be maintained by the Department's TSB.

It is the responsibility of departmental management to implement, as resources dictate, the training standards established by the committee.

41030.7 Division Training Coordinators

It is recommended that division training coordinators be appointed to assist the EDP Training Committee in inventorying employee skills, assessing training needs, and developing training schedules.

41030.8 Revisions

The Chief, ISD or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

41030.9 References

None.

ARTICLE 4 — GENERAL INFORMATION AND POLICY

Revised October 17, 1994

42010.1 Policy

It is the policy of the Department to create and maintain an annual ITS plan. This plan, prepared by ISD (see DOM 43010.3, Information Management Planning, Responsibilities) and approved by the MIS Committee, shall be the primary basis for structuring the use of ITS in CDC.

The annual departmental ITS plan shall, at a minimum, contain strategy for the use of:

- State data centers for departmental critical systems.

- Distributed systems for departmental critical systems.
- Microcomputers for departmental critical systems.
- Departmental telecommunications and networking systems.
- Facility PBXs for data.
- Local area networks.
- Modems.

42010.2 Purpose

The purpose of this policy is to disseminate the framework for the decision-making process used by the Department in deciding to apply automated solutions to the Department's operations, accounting, and communications problems.

42010.3 ITS Selection Criteria

It is the intent of the Department to employ the following factors when deciding whether to use CDC ITS resources to develop, design, and implement a critical departmental information system:

- The priority of the ITS request (see DOM 43000).
- The relationship to the Department's goals and objectives.
- The extent to which the application is critical to accomplishment of the Department's goals and objectives.
- The risk analysis report (see DOM 49000).
- The results of a pilot project.

The Department's strategies for use of such technologies shall be utilized to determine the design of the approved information system and the choice of hardware, software, and communication.

42010.4 ITS Selection Process

The Department's vehicle for selection of technological alternatives is the FSR. When preparing an FSR, the above selection criteria shall be utilized as a basis. When automation is determined to be the approach to solving a business problem, the Department shall choose the automated system which best accomplishes the tasks involved.

The Department currently maintains a multi-tiered automation platform that offers a wide spectrum of hardware/software choices and which provides several databases accessible to applications for data sharing.

A significant feature of automated systems is the ability to share data. Benefits of data sharing include the saving of valuable input time and, in many cases, may solve cost justification problems by reducing or redirecting data input time and associated personnel years.

There are many automation platforms available for expansion in the Department. However, there are also many elements listed in the selection criteria that lead to the appropriate solution. Regardless of the business problem, selection criteria, or platform (hardware/software) involved, State policy requires that the FSR shall show a cost reduction, a viable cost avoidance, increased revenue, operational necessity, or be the result of a legislative mandate before approval of the concept can become a funded project.

In many instances, the FSR may have a concurrently associated pilot project to provide specific performance, cost, and technological justification for the continuance of the project.

42010.5 ITS Pilot Projects

Pilot projects are scaled down versions of an overall project. They are intended to provide information on cost savings/avoidance, technology use, or performance of bench marking in order to justify implementation of the full project. A pilot project is a subset of the overall project and is subject to the same approval process as the full project.

Many projects are approved through the Office of Information Technology (OIT) and the FSR process contingent upon pilot justification of the project.

The typical contents of a Pilot Implementation and Evaluation Plan include the sections and contents described below:

Program Performance Improvements

This section defines the programmatic functions to be included in the pilot. It should include a description of the current processes, a description of the new processes, and a plan that includes quantified measurements for evaluating before-and-after program performance.

Physical and Technical Characteristics

This section describes the physical and technical characteristics of the pilot. It shall include descriptions of sites, equipment, software, and telecommunications as well as any other technical resources that are needed to complete the pilot.

Information Requirements

This section defines the informational processing requirements of the pilot. It should include definitions of data inputs (source, type, volume, timing, media, files, edits, etc.), processes (response times, interfaces, security, etc.), and outputs (reports and displays).

Security Requirements

This section addresses the process to be used to determine the potential problems and risks, the controls necessary to safeguard the information hardware and software of the pilot, and the fully-implemented system. Typically, a risk analysis as described in DOM 49030 shall supply the necessary information. The completion of this requirement is especially important since necessary security controls can often increase the required budget.

Financial Requirements

This section contains an estimate of all costs associated with the pilot phase of the project. Project accounting shall be defined so that actual pilot costs and benefits can be compared against estimates, and then used as a basis to refine full implementation estimates.

Operational Recovery Requirement

This section addresses the process to be used to determine the operational recovery requirements. A pilot project shall have an operational recovery plan just for the pilot, and shall address the issue of operational recovery of the proposed fully-implemented system. Often, operational recovery processes add to the overall cost of the project. All critical departmental systems shall have an operational recovery plan as part of their implementation (see DOM 44000).

Management Plan

This section contains a pilot management plan. The plan shall include:

- Pilot responsibilities.
- Pilot schedule.
- Pilot reporting and review.

Any special requirements shall be identified such as training, conversion, or impact on existing operations.

At the end of the pilot and before continuing with the project, a Post Implementation Evaluation Report (PIER) shall be completed and submitted to either the departmental MIS Committee or OIT for review. The pilot PIER shall contain an assessment of programmatic performance during the pilot. The results of the pilot PIER shall be used to re-evaluate the analysis completed for the original feasibility study and, if necessary, be used to make changes to the project FSR.

Once the pilot PIER is approved and any necessary changes are made to the original FSR, the pilot PIER shall be reviewed and the project may be initiated upon its approval.

42010.6 Determining Priorities on ITS Requests

One of the criteria for project selection is the priority of the ITS request. To assist in decision-making, the following schema shall be utilized when assigning a priority to a particular request for information system resources: If multiple requests exist with the same priority, each division submitting requests shall determine the order of further prioritization. For example, if there are four priority 3.1 requests then these four requests should be renumbered as 3.1.1, 3.1.2, 3.1.3, and 3.1.4 in order of further priority.

The following is a description of several different levels of priorities. These priorities can be thought of as an initial rationale for assignment of ITS design, development, and maintenance resources. Each prospective project shall be assigned one of the following priorities prior to its presentation before the MIS Committee:

Priority 1

- This priority level is exclusive to the maintenance of computer programs that have been designed, implemented, and installed. Resources used in this area are for the purpose of keeping existing computer-based systems functional. This priority includes routine maintenance. Any changes to production systems requiring more than 32 person-hours shall not be considered as maintenance, but as a new request which must be justified.

Priority 2

- Those resource requirements over which the Department has little control. Responses to legislative action, requests from the Governor or the agency, and requests from local law enforcement for critical information are all examples of projects that are Priority 2.

Priority 3

- An ITS request shall be Priority 3 if the implementation of the proposed computer-based system will result in a measurable benefit to the Department. Most requests for information system resources fall within this area.

42010.7 Revisions

The Assistant Director, OOC, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

42010.8 References

DOM §§ 43000, 44000, and 49000.

ARTICLE 5 –EDP STANDARDS

Revised April 9, 2002

42020.1 Policy

It is the policy of the Department to promote standardization in its information management planning and operations through adherence to applicable American National Standards Institute (ANSI), Federal Information Processing Standards (FIPS), and State standards and guidelines. All proposed application or information technology activities shall be evaluated to ensure that all hardware, software, and communications platforms comply with ANSI, FIPS, and State standards and guidelines.

42020.2 Purpose

The purpose of this Policy is to facilitate the inter-organizational sharing and exchange of equipment, data, software, and personnel. The use of these EDP standards shall also facilitate communication:

- Between the Department and other State agencies.
- Between the Department and its EDP vendors.
- Between the Department and its EDP information providers/recipients.
- Among the various organizational units within the Department.

Adherence to established EDP standards should result in improved communication, improved product quality, decreased development time and costs, improved project control, and reduced maintenance costs.

42020.3 Computer Programming Language Standards

Where custom programming is needed, the Department requires the use of vendor-supplied programming languages which are departmental standard languages. The language chosen for development shall be consistent with the requirements of the application and platform for which it is intended.

- For new system development on minicomputer or mainframe platforms, a high level language shall be used wherever feasible. In this case, high level languages include either a fourth generation language such as Oracle or a Computer Assisted Software Engineering (CASE) tool integrated with a COBOL code generator.
- Where a high level language is not feasible or where maintenance shall be performed on applications already written in COBOL, the COBOL programming language shall be used.
- In the personal computer (PC) area, application programming shall use either a language or compiler compatible with the dBASE standard, a fourth generation language for the PC, or a CASE tool integrated with a COBOL code generator.

Use of vendor-supplied data base management, report generation, and file manipulation packages shall be considered in the design of ITS. For data management on all platforms, the use of a vendor-supplied relational data base management system compatible with structured query language (SQL) is recommended. The in-house development of data base management or file manipulation software is strongly discouraged and only permitted where there is no other alternative.

Normally, high level languages possess their own query language and report generation software. Wherever possible, the query language and report generator provided with the high level language shall be used. In situations where such software is not provided with the high level language or will not meet the application's needs, third party query languages and report generation software can be chosen from the wide variety of software supplied by vendors.

42020.3.1 Application Generators

The Department encourages the investigation and use of application generator software.

Application generators are integrated fourth-generation language tools which permit an entire application to be generated. The most useful full-function application generators support a wide range of integrated components including a data base management system (DBMS), data dictionary, security facilities, analysis tools, query language, report generator, documentation generator, screen painter, prototyping facilitator, graphics generator, decision support or financial modeling tools, multiple end-user interfaces, high-level procedural language, data definition language, distributed processing facilities, testing tools, a micro-to-mainframe communications link, and a separate version of the tool for a personal computer.

Application generators for EDP professionals generally include a very high-level procedural language that is used to specify logical operations. These tools are usually integrated with a full-function DBMS that supports both relational and other data structures.

42020.3.2 Operating Software

It is the Department's policy that standard, unmodified, vendor-supplied and maintained software aids be used in lieu of developing unique programs. The objective is to minimize and control the development of specialized programs that allocate, schedule, and control the central processing unit, memory, peripherals, communication, and data storage and retrieval.

42020.3.3 Application Packages

It is the Department's policy that all feasibility studies shall have one alternative addressing the availability, usability, maintainability, and cost-effectiveness of prewritten and tested application programs in lieu of developing major programs in-house. The PC Policy in DOM 48010 addresses PC application packages. The objective is to minimize the development time and costs of major application programs when such programs are available from other sources. For some custom applications, however, in-house development may be the most viable alternative.

42020.4 Systems Development Life Cycle

The Systems Development Life Cycle (SDLC) is a systematic approach to software development that defines development phases. It begins when a software product is conceived and ends when the product is in production and being maintained. It also specifies the activities, products, verification procedures, and completion criteria for each phase. It is an effective engineering management tool that can be used to help ensure that a delivered product is correct and meets the user's needs.

The Department advocates use of the SDLC approach to software development, whether the platform is mini or mainframe. However, if the system being developed is a standalone PC system, development phases may be combined or omitted so long as the delivered product meets the user's needs.

The Department has included the following phases in its SDLC: Concept Phase, Requirements Phase, Design Phase, Development Phase, Testing Phase, and Operation and Maintenance Phase.

42020.4.1 Concept Phase

The Concept Phase is the initial phase of system development during which user needs are described through documentation. The user group is formed during this phase. Examples of the documentation include a statement of needs, advance planning report, project initiation memo, feasibility studies, system definition documentation, regulations, and policies and procedures relevant to the project. Deliverables for this phase include:

- The project charter.
- The project management plan.
- The initial project file.

42020.4.2 Requirements Phase

The Requirements Phase is the period of time in the life cycle during which the requirements for a software product, such as functional and performance capabilities, are defined and documented. Major deliverables include the Software Requirements Specification documentation and the Baseline Report.

42020.4.3 Design Phase

The Design Phase is the period of time in which the designs for architecture, software components, interfaces and data are created, documented, and verified to satisfy requirements. Major deliverables include the Detailed Design Specification, the Test Plan, the Implementation Plan, the Users' Manual and Procedures Manual, and the Training Plan.

42020.4.4 Development Phase

The Development Phase is the period of time in the development life cycle during which a software product is created from design, documentation is tested, and errors are corrected. Major deliverables of this phase include system

documentation, program documentation, program code, and test results documentation.

42020.4.5 Testing Phase

The Testing Phase is the period of time in the life cycle in which the software product is evaluated by users and technical staff to determine whether requirements have been satisfied. Tests performed include the Requirements Test, the Operational Environment Tests, the Acceptance Test, and the Pilot Test.

42020.4.6 Operation and Maintenance Phase

The Operation and Maintenance Phase is the period of time in the life cycle during which a software product is used in its operational environment, monitored for satisfactory performance, and modified as necessary to correct problems or respond to changing requirements. The Post Implementation Evaluation Report (PIER) is completed during this phase.

42020.5 User Computing Within CDCR

The standards addressed in DOM 42020.3 above, Computer Programming Language Standards, apply to end-users as well as EDP professionals, although the end-user shall not use procedural or third generation languages and shall restrict any programming activity to the personal computer.

42020.5.1 Personal Computer

The personal computer is meant to be a productivity tool to assist the user in fulfilling regular professional responsibilities.

42020.5.2 Database/Spreadsheet

A user-developed system is defined as a database or spreadsheet that is created, accessed, or updated with an off-the-shelf software application.

42020.5.3 Management Approval

Approval shall be obtained from appropriate division management prior to expending any resources on a user-developed system that is used in an official capacity by any departmental personnel.

42020.5.4 Standard EDP Documentation

In order to ensure continued operation of user-developed systems, documentation shall be provided. Documentation shall include:

- A list of application software used (e.g., dBase, Foxbase, Lotus, Quattro, etc.).
- System requirements.
- A user manual to explain:

Where the system is installed (PC location, drive, directory).

- How the system is started.
- Any macros or batch files used.
- Data entry procedures.
- Report generation.
- Backup procedures.
- File descriptions for each file used in the system:
  - File name.
  - File type (report, label, index, memo, database, spreadsheet).
- Structure of any data files:
  - Description of each data field.

Refer also to DOM 48010, Departmental Workgroup Computer Policy.

42020.6 Inmate Access to Computing

Computers are used in inmate academic/vocational education training programs. It is essential that the security of the facility be maintained and that no unauthorized communication is made by a computer to another computer or to an electronic mail device. In addition, data integrity and systems security shall be maintained at each work location. Each Warden, RPA, and Associate Director shall be responsible for computer resources and information security within their respective facility or division.

Each Warden shall designate an Information Security Coordinator who shall not be at a level below AISA. This coordinator shall report any security violations, concerns, or questions to the Warden and the divisional Information Security Officer/Coordinator. The divisional coordinator shall report security incidents to the Department Information Security Officer (ISO).

No inmate shall have any computer, modem, or terminal in possession within the facility. There shall be no inmate access to a computer outside the inmate's authorized work, vocational, or educational areas.

It is the Department's goal to eliminate the use of inmates as programmers for applications used by the Department outside of the PIA. Within PIA, inmate program development shall be controlled strictly by PIA headquarters.

For those facilities now utilizing inmates to develop and maintain programs, a plan shall be developed to strictly monitor this activity until it can be discontinued.

Outside of PIA, each facility now using inmates for the development of programs for Department use (i.e., not part of an inmate education program) shall include the following procedures as part of its monitoring plan:

- All inmate computer program development shall be under the supervision of the AISA in a controlled, designated area.
- All inmate-developed programs shall be written in either dBase, Foxbase, or Clipper. Existing programs shall be converted to one of these languages.
- Source code and documentation shall be reviewed by the ISA before final compiling.

All facilities with inmates accessing computers in any capacity, including inmate education programs, shall comply with the following procedures:

- Each computer shall be labeled to indicate whether inmate access is authorized.
- Areas where inmates are authorized to work on computers shall be posted as such.
- There shall be no communication capabilities such as telephone, computer line, or radio communication devices in the area.
- Inmates shall not have access to utility programs such as Mace, Norton Utilities, or PC Tools.
- Inmates shall not have access to the MS-DOS commands DEBUG, ASSIGN, and ATTRIB.
- A copy of all facility personal computer-based programs, source codes, and documentation shall be forwarded to and maintained by ISD.
- Inmates performing data entry or word processing in an authorized education or work production area should be supervised by staff persons able to identify and use the computer operating system, software, and application used on the equipment under their supervision.

The Division of Adult Institutions shall develop and maintain a system to track inmates who have documented, sophisticated computer expertise or histories of computer fraud or abuse. This identified group of inmates shall not be assigned duties involving the use of personal computers.

Inmates shall not have access to any computer containing sensitive or confidential information. In addition, computers containing sensitive or confidential information shall have appropriate hardware or software security measures installed.

Inmates shall not remove diskettes from authorized work areas. An inventory and appropriate controls shall be maintained on all diskettes. Diskettes for inmate use shall be labeled "For Inmate Use." Reports and other printed output from inmate-utilized computers shall be reviewed closely by staff and appropriate distribution of such output shall be monitored.

Unit managers currently utilizing inmates for programming applications shall have a plan for the completion of user and programming documentation. This documentation shall be approved and used by the facility AISA for program auditing/maintenance. Once approved, a copy of the plan shall be forwarded to EIS. The plan shall then be forwarded to the ISO. In the absence of an approved plan, all programming and editing features shall be removed from computers accessed by inmates.

42020.7 Revisions

The Assistant Director, OOC, or designee shall be responsible for ensuring that the contents of this Section are kept current and accurate.

42020.8 References

OIT, Information Management Guideline: A Manager's Guide to End User Computing.

DOM § 48010.

ARTICLE 6 — QUALITY ASSURANCE AND QUALITY CONTROL

Revised October 17, 1994

42030.1 Policy

It is the policy of the Department to provide Quality Assurance (QA) and Quality Control (QC) functions to ensure the usability and effectiveness of all EDP applications and processes.

42030.2 Purpose

The purpose of the QA function is to facilitate the continuous review and improvement of processes which underlie the creation and maintenance of automated systems and databases. The purpose of the QC function is to implement methods and practices that allow EDP products and processes to be measured against predefined standards. Together, QA and QC ensure that automated systems and their products better meet user needs.

42030.3 Responsibilities

CDC recognizes that maintaining adequate, correct and current offender data is critical to departmental operations that directly affect staff, inmate, and public safety. OISB, in the ASD, is responsible for major current, proposed, and future statewide offender ITS. QA procedures to be applied to these departmental ITS include:

- Continual monitoring of the validity and currency of data contained in offender ITS;
- Establishment of methods to identify errors or inadequacies in these data; and
- Development of appropriate procedures and solutions to correct inaccuracies or out-of-date data.

The OISB does not directly implement most procedures and solutions. Rather, once a problem has been identified the OISB provides the owners of the data with tools and procedures aimed at eliminating the problem. After the owners of the data have implemented these tools and procedures, the OISB provides ongoing review of the data to ensure its accuracy, currency, and completeness.

A QA council shall be established to ensure that departmental QA policies, standards, and procedures are implemented and maintained. Responsibility for implementing QA resides with each entity (i.e., division, branch, or unit) that develops and maintains systems.

QA Council

The QA council shall be comprised of the departmental Information Security Officer (Chairperson) and representatives from each division responsible for the development and maintenance of ITS. The QA council shall:

- Develop departmental QA policies, standards, and procedures.
- Develop and implement an annual QA plan in support of the Department's strategic plan.
- Ensure that systems developed or maintained in the Department adhere to CDC QA/QC standards and procedures.
- Support programs that educate CDC staff in the importance of quality concepts and in the tools, techniques, methods, and practices that facilitate QA and QC.
- Act as a source of information on processing quality data and on the need for continued commitment to an improvement effort.
- Review industry standards (e.g., ANSI/IEEE, FIPS) to facilitate the development of departmental EDP standards.

The QA council shall meet quarterly or as needed.

Division/Branch/Unit

Accountability for QA and QC is fixed on a system by system basis. See DOM 47000, Departmental Systems, for ownership designation and fixed responsibility for QC.

OISB is responsible for data integrity in major, statewide offender ITS.

In fulfilling QA/QC responsibilities each entity shall, where applicable, ensure that:

- ITS projects are reviewed during all phases of the systems development life cycle (SDLC).
- Data integrity is developed and maintained, both in the SDLC and by the unit designated responsible for QC, on each application or database.
- User requirements are well-defined (for systems development or maintenance projects), all objectives of the work effort have been met, and results are appropriate keeping in mind each project's overall objectives.
- The ITS processes are monitored and measured for the purpose of improving these processes.
- Quality improvement programs are established and quality concepts are promoted throughout Department branches that develop and maintain ITS.

42030.4 Definitions

Acceptance Testing

Testing that insures a computer system meets the needs of the organization and the end-user.

Client (User)

The individual or organization that utilizes a product.

Correctness

(1) The extent to which software conforms to its specifications and standards; (2) the extent to which software is free from design and coding defects (i.e., "fault-free"); and (3) the extent to which software meets user expectations.

Cost of Quality

The cost of quality for a product is the sum of prevention, detection, correction, and client costs. Prevention cost is the total cost incurred during product development prior to general release. Detection, correction, and client costs are post-release costs associated with reworking due to defects. QA shall be considered cost-effective when post-release costs are reduced by an amount greater than any increase in prevention costs resulting from the inclusion of QA in the development process.

Data Base Integrity

The accuracy, completeness, and timeliness of information contained in a database.

Defect

A variance from specifications/standards or attribute/function not contained in the software requirements specifications.

Defect-Prone Process

A process/activity during which a high number of defects occur.

Desk Checking

An informal evaluation technique in which the person who developed a unit of code inspects it visually to identify possible errors or violations of development standards.

Failure

Inability of a product or service to perform its required functions within previously established limits.

Integration Testing

Testing performed on groups of modules to ensure data and control are passed properly between modules.

Long-Term Capacity Planning

The objective of long-term capacity planning is to develop methods and means for ensuring that hardware, system software, communications, and system design shall meet the long-term objectives for additional processing required by new applications, integration of new processors and platforms, and new generations of software. This plan encompasses a five- to seven- year period and is designed to help determine budget requirements and goals for the Department.

Post Implementation Evaluation Report

The review of a computer, computer system, or computer network that has been in operation for at least six months and no longer than two years for the purpose of matching the requirements of the system against what has been produced, so as to ensure that stated requirements have been met.

Problem Reporting/ Tracking

A process of reporting outstanding problems, having them assigned for resolution, and closing them out when the user has been notified that the problems have been solved.

Process

The work activities that produce products, including the efforts of people and equipment.

Product

The output of a process including the goods and services produced by individuals and the organization.

Quality

The extent to which a product meets the expectations and requirements of the user.

QA

(1) A staff function designed to support line management in performing the QC function. As such, QA identifies those processes, both good and bad, that affect quality, and is used to advise management of such effects. A management decision may then be necessary to ensure that QC techniques are implemented and maintained; and

(2) The function that uses measurement and analysis to continually improve processing, procedures, and standards so that management can be "assured" of their staff following such methods, procedures, and standards, as well as their ability to produce products that meet specified requirements.

QC

(1) The collection of activities to ensure that defects are neither made nor implemented. While QA monitors the processes involved in the production cycle, QC is an integral part of work and is the responsibility of each employee; and

(2) A line function used to measure quality associated with specific products or services. QC is the responsibility of each ITS area and is the function responsible for the quality of the work being done within a specific area or for a specific project.

Quality Improvement Program

A program designed to reduce the number of defects produced.

Regression Testing

Testing applied after changes have been made to ensure that no unwanted changes have been introduced.

Requirement

The specification(s) for satisfying a user need; is associated with a standard by which the satisfaction of that need can be measured.

Resource Management

The determination of current and short-term needs for hardware, system performance, and communications, and the allocation of such resources to meet the overall goals and current short-term plans of the Department. Resource Management requires the gathering of data about new processing needs and applications not addressed in long-range planning, as well as any other information that impacts current system resources.

System Testing

A generic term that differentiates various types of higher order testing from unit testing.

Total Quality Management

Consists of continuous process improvement activities involving everyone in an organization--managers and workers--in a totally integrated effort toward improving performance at every level. This improved performance is directed toward satisfying such cross-functional goals as quality, cost, schedule, mission, need, and suitability. Total Quality Management, or TQM, integrates fundamental management techniques, existing improvement efforts, and technical tools under a disciplined approach focused on continuous process improvement. The activities are focused ultimately on increased client/user satisfaction.

Unit Testing

Testing performed on a single, standalone module or unit of code.

Validation

The process of comparing a product in any stage of its development with specified requirements in order to determine whether the correct product is being produced.

Walk-Through

A review process in which a designer or programmer leads one or more members of the development team through a segment of documentation or code that he or she has written, and other team members ask questions and make comments about technique, style, possible errors, violation of development standards, and other issues.

42030.5 Revisions

The Assistant Director, OOC, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

42030.6 References

Quality Assurance Institute: Effective Methods For Quality Assurance In Information Systems.

DOM § 47000.

ARTICLE 7 — INFORMATION MANAGEMENT PLANNING

Revised October 17, 1994

43010.1 Policy

The Department has established a management planning process that is consistent with the needs, resources, and use of information technology within the Department. In compliance with the SAM 4900.2, the established management planning process:

- Is consistent with the current statewide policies contained inSAMand current management memos for managing information and information technology.
- Is linked to and supportive of CDC's overall program planning and budgeting processes.
- Involves CDC executive management and program managers, as well as those who are responsible for the use, operation, and support of ITS.
- Addresses current and projected relationships among the various aspects of information technology employed by CDC, including equipment (such as mainframes and minicomputers, personal computers, and office systems), software (such as computer languages, including fourth generation languages, and applications packages), and telecommunications.
- Relates current and planned uses of information technology to the information required for the accomplishment of CDC's mission and key programs.
- Considers means for ensuring the continuing availability of the information required to support critical programs in the event of disaster, or other unforeseen events resulting in an interruption of CDC's regular systems operation.

43010.2 Purpose

Planning includes identifying needs and opportunities, defining objectives, and determining appropriate means of achieving those objectives. The purposes of information management planning are to:

- Find ways that information technology can improve the effectiveness of CDC programs.
- Analyze the costs and benefits of information technology and allocate resources systematically.
- Clarify CDC's priorities and be able to react to changes with a minimal amount of disruption.
- Improve communication among executive managers, staff responsible for information technology, and the users of the programs.
- Provide managers with a long-term perspective on current problems that simplifies making decisions and solving problems.

In addition, planning requirements are intended to provide the Office of Information Technology (OIT) and other control and oversight organizations with the basic facts those organizations require to carry out their responsibilities concerning the use of information technology in State government.

43010.3 Responsibility

It is the responsibility of ISD to develop and maintain a departmental strategic plan. This plan shall be approved by the MIS Committee. Once approved, this plan shall serve as the road map for planned automation efforts within the Department. This plan shall be utilized to link divisional planning efforts to the goals and objectives of the division and Department. The MIS Committee shall ensure that all projects under its responsibility are consistent with and do not conflict with other planned efforts. Compatibility and connectivity shall be the shared vision of all planning.

43010.4 Information Management Planning Infrastructure

CDC has developed a formal structure for planning which includes an MIS Committee and an ongoing planning process that involves analysis, evaluation, and review of proposed projects. This project review, reporting, and evaluation process is covered in DOM Subchapter 44000, Project Review, Reporting and Evaluation. Alternately, this subchapter describes the MIS Committee, the MIS Support Unit (MIS-SU), ISD, and the role each plays in the management planning process.

MIS Committee

The MIS Committee, whose members represent the divisions within CDC and the PIA, is responsible for executive leadership and strategic planning in seeking out opportunities to employ information technology for the achievement of the Department's mission, goals, and objectives. The MIS Committee assesses all proposed ITS projects (ranked according to their importance to the Department's mission) to assure conformance with the Department's mission statement, strategic plan, and key programs. The committee also reviews and approves the Department's Information Management Annual Plan (IMAP) and endorses future

needs identified in long-range planning documents. DOM 41020.3 describes the role of the MIS Committee.

ISD

ISD is responsible for development and maintenance of the overall strategic plan of the Department. This plan shall be the result of compiling all divisional automation needs into a single document for the prioritization of projects and alignment with the budget by the MIS Committee.

ISD is also responsible for maintaining and updating the IMAP. This includes: working with the user to develop appropriate documents for inclusion in the IMAP for those projects reportable to OIT, ensuring that the appropriate reportable project forms are completed, notifying the user once a project has been approved, whether it is delegated or non-delegated, maintaining copies of all reports, and, as appropriate, acting as a liaison between OIT and CDC project management concerning reporting requirements throughout the life cycle of the project.

MIS-SU

The MIS-SU provides functional support to the MIS Committee by coordinating MIS Committee meeting agendas, coordinating the review of proposed ITS projects, preparing annual updates for the Department cabinet on all CDC automation efforts for the current year as well as strategic planning for the coming year, and participating in the development of presentations for the committee addressing current technical innovations and coordinating the review of information system concepts to ensure compliance and consonance with the budget cycle. Refer to DOM 41020.4 for more details on the role of the MIS-SU.

43010.5 Information Management Planning Process

The Department uses the MBO approach for planning information management. The Department's mission and philosophy statement were developed based on MBO principles, and resulted from many planning sessions held to enlist ideas from numerous levels, disciplines, and segments within the Department.

Each Division formulates its own goals and objectives using departmental goals and objectives as the foundation for the effort. The CDC ITS planning process originates with the development of the strategic plan (see also DOM 43010.3). MBO goals and objectives are developed to structure the Department's efforts to achieve the purposes specified in the strategic plan. The establishment of such goals and objectives allows the identification of automation opportunities consistent with the plan, and the planning process then provides for the development of various concept statements to enable articulation of methods that may be used to benefit from the identified automation opportunities. All automation concept papers are reviewed by the MIS Committee and, if approved, become part of the IMAP. Implementation of an automation concept that requires increased or new source funding may require the preparation of a Budget Concept Statement, and a BCP may also be necessary. Establishment of certain automation projects as specified in this Chapter shall require prior approval of an FSR.

ISD shall provide the general guidelines for objectives that require automated solutions. The resulting document, the Information Systems Budget Concept Statement (IS-BCS), is submitted to ISD and the MIS-SU for review and recommendations.

ISD shall coordinate development of the IMAP, and shall maintain it to ensure that a vision of connectivity and compatibility is followed. Redundancy of data input is another area of concern, and this plan shall help ensure that a planned automation effort is coordinated within the department. Duplication of automation efforts is a costly and time-consuming waste. The IMAP shall serve as a road map for automated efforts.

The MIS Committee shall measure proposed projects against CDC's, mission and established departmental priorities so as to best prioritize and approve proposed EDP projects.

43010.6 Revisions

The Assistant Director, OOC, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

43010.7 References

SAM § 4900.2.

DOM §§ 44000, 41020.3 and 41020.4.

ARTICLE 8 — PROJECT INITIATION AND APPROVAL

Revised October 17, 1994

43020.1 Policy

It is the policy of the Department that information system proposals shall receive departmental and, as required, control agency approval before project development can proceed.

43020.2 Purpose

The purpose of this policy is to ensure that the Department is in compliance with all control agency requirements. The ultimate authority for approval of information technology projects lies with the Office of Information Technology (OIT), but it is the intention of the Director of OIT to delegate such approval authority selectively, to the maximum extent practicable, to the departmental director. Refer to SAM 4819.34 for the factors considered by OIT in determining whether a project can be delegated.

43020.3 Project Initiation and Approval Process

ITS proposals requiring a change in the Governor's budget for funding purposes shall receive departmental and control agency review and approval before project development can proceed.

43020.3.1 Requests Requiring a Change in the Governor's Budget

If funding for a project is already available, departmental and control agency review and approval is still necessary but the approval process is somewhat different and is discussed in DOM 43020.3.2.

Early each calendar year, MIS-SU shall distribute a memorandum to CDC Executive Staff, Wardens, and RPAs detailing the IS-BCS request process for the fiscal year beginning approximately 18 months later. This memorandum shall include a timeline containing significant deadlines which shall be met in order for a request to proceed through the approval process. The following is a general discussion of this process.

ITS proposals shall be presented to the MIS Committee utilizing the IS-BCS format. The purpose of this format is to provide sufficient information to departmental executive staff to allow for a determination of whether the proposal warrants further development as a BCP. BCPs are discussed in DOM 21010 and SAM 6100.

Refer to the following instructions when completing the IS-BCS and note that the format shall not exceed two pages in length including any supporting documentation. Requests out of compliance with the established format and instructions shall be returned to the requester without consideration.

Statement of

Indicate as concisely as possible what problem exists or what level of service is not being provided.

Description of Existing Operation

Describe the current operation including a description of the criticality of the data, how or whether it is currently being collected, and the current staffing allocated to its collection, maintenance, and analysis.

Adverse Effects of Continuing Existing Operation

Specify what adverse effects would be experienced by continuing the existing operation. These effects should be quantified to the extent possible.

Alternatives for Solving the Problem

Describe several alternative methods considered to address the problem. List the pros and cons of each alternative.

Recommended Solution

Select an alternative. Discuss how its implementation would alleviate those problems identified above. Quantify the staffing or all other resources needed to implement the proposed change.

Identification of Needed Resources (Estimate of Cost/Benefits)

Although a detailed cost/benefit analysis cannot be provided until an FSR is completed, the requester should be able to provide a conservative estimate of any real savings or costs associated with the ITS concept.

IS-BCS's shall follow the normal chain of command for divisional approval prior to review by the MIS Committee.

Timeframe

Process

December

MIS-SU staff coordinate the presentation of the annual update to the Cabinet detailing all major CDC automation efforts during the previous year and strategic planning for the coming year.

Late January

IS-BCSs that have received division approval are submitted to MIS-SU for inclusion on the March MIS Committee meeting agenda. MIS-SU and ISD staff review the IS-BCS in terms of its conceptual integrity and consistency with the Department's approved strategic plan. ISD staff review the IS-BCS to assess its technical feasibility. MIS-SU and ISD staff each formulate a recommendation addressing the IS-BCS for MIS Committee deliberation.

Early March

The MIS Committee reviews the IS-BCS and recommendations to determine whether an FSR and BCP should be developed.

Timeframe

Process

Late March

If the concept is approved at the MIS Committee meeting, the IS's FSR/BCP development may begin (see SAM Section 4920). Requester submits a New Reportable Project Form to ISD to include the project in the departmental Information Management Annual Plan (IMAP).

Also due to ISD at this time is the project's draft FSR.

Early June

ISD submits the IMAP to the MIS Committee for review and approval. BCPs and departmentally approved FSRs shall be submitted to OBM for initial review.

Mid June

Departmentally approved FSRs are submitted to the OIT for review.

Late July

The Department conducts hearings on BCPs from all departmental program areas to determine which proposals will go forward to Agency for review and approval. The IMAP is submitted to the OIT for a determination of the project's reporting requirements through its review of the IMAP. See SAM 4900 and DOM 43020.4 for specific information and instructions.

Early August

Agency conducts its review of departmentally approved BCPs to determine which proposals will go forward to the DOF for review and approval.

September

DOF conducts its review of Agency-approved BCPs to determine which BCPs shall result in actual project development funded by a change in the Governor's budget. DOF decisions are usually distributed by the end of December.

Project development can begin upon DOF's approval of the BCP.

43020.3.2 Projects to be Funded with Existing Monies (No New Positions)

ITS proposals to be funded with existing monies (no new positions) shall receive departmental and, if necessary, control agency review and approval before project development can proceed.

Refer to DOM 48010.2 for information regarding the procurement of personal computer equipment.

ITS proposals shall be presented to the MIS Committee utilizing the IS-BCS format. The purpose of this format is to provide sufficient information to departmental executive staff to enable a determination of whether the proposal warrants further development (see DOM 43010.1.1).

The IS-BCS shall follow the normal chain of command for divisional approval before it is reviewed by the MIS Committee.

After the IS-BCS has received divisional approval, it shall be submitted to MIS-SU for inclusion on the MIS Committee agenda. See DOM 41020 for additional information regarding the MIS Committee and MIS-SU.

If the IS-BCS receives MIS Committee approval and meets the requirements of a reportable project, the requester shall submit a New Reportable Project Form to ISD to include the system in the departmental IMAP. OIT shall determine the project's reporting requirements through its review of the IMAP. See SAM Section 4900 and DOM 43020.5 for specific information and instructions.

After the IS-BCS receives MIS Committee approval, the project's FSR can be prepared (see SAM Section 4920 for specific information and instructions). Upon completion and divisional approval, the FSR is due to ISD for technical review and approval.

Depending on the reporting requirements established for the project, the departmentally-approved FSR shall next be submitted to OIT for review and approval. See SAM Section 4900 and DOM 43020.5 for further details.

Project development can begin once the FSR has received departmental and, if required, OIT approval.

43020.3.3 Non-reportable Projects Under $50,000 to be Funded With Existing Monies (No New Positions)

Non-reportable information technology projects under $50,000 that are funded through redirection do not require submission of an IS-BCS. Instead, a CDC Internal Project Summary Fact Sheet (IPSFS) must be completed and forwarded to the ISD Project Initiation Unit (PIU) for review. The IPSFS must then be presented to the MIS Committee for approval. Once approval is obtained, the PIU shall forward a copy of the approval letter to the project manager and maintain a copy in the ISD files.

43020.4 Information Management Annual Plan (IMAP)

The IMAP represents the results of CDC's planning process. It identifies those projects for which resource commitments are anticipated and, in effect, summarizes CDC plans, projects, and other activities associated with its use of information technology.

SAM Section 4900 requires that each agency involved in information technology activities prepare an IMAP.

43020.4.1 IMAP Composition

The IMAP consists of three parts:

- Part A: Overview.
- Part B: Information Technology Activities.
- Part C: Exhibits and Supporting Documents.

43020.4.1.1 Part A - Overview

Part A contains a brief description of the agency's mission, its current problems and opportunities associated with information management, and its strategy and objectives for the use of information technology.

43020.4.1.2 Part B – Information Technology

Part B provides an overview of current and proposed development projects and potential acquisition activities, with particular emphasis on those projects and activities that are relatively costly, require a BCP, or meet any of the other special criteria described in SAM Section 4902.1.

43020.4.1.3 Part C - Exhibits and Supporting Documents

Part C contains Documents that supplement the information in Parts A and B of the IMAP by providing details about the agency's organization of information management and its available resources.

43020.4.2 IMAP Purpose

The purpose of the IMAP is to ensure that CDC is systematic in identifying and satisfying its information requirements and provides OIT and other control and oversight agencies with the basic facts those organizations require to carry out their responsibilities regarding the use of information technology in State government.

43020.4.3 IMAP Responsibilities

ISD is responsible for assembling and maintaining the IMAP. ISD develops IMAP - Part A and the support documents contained in Part C. Part B of the IMAP consists of New Reportable Project Forms that are completed by the project teams involved in the information technology projects, and summaries of project status for any major projects.

43020.4.4 Reportable Projects

SAM Section 4902.1 lists the criteria used to determine if a project is considered reportable. Reportable projects require completion of a New Reportable Project Form. This form is included in Section B of the IMAP and provides OIT with information on the proposed project. OIT uses this information to determine whether approval authority for the project shall be delegated to CDC or if OIT shall retain the approval authority.

All proposed projects that do not meet the criteria in SAM Section 4902.1 are considered non-reportable projects. The costs of agency development or new acquisition projects, whether reportable or not, shall be included in the Agency Information Technology Costs spreadsheet included in Part C of the IMAP.

43020.4.4.1 Definition of Reportable Project

A Reportable Project is defined as a planned development activity or the planned acquisition of a new or enhanced information technology capability (as defined in SAM Section 4819.2) which meets one or more of the following criteria:

- The project involves total estimated development or acquisition costs that are greater than the cost threshold established for the agency (see DOM 43020.4.4.2 for further information on cost thresholds).

- The project involves a budget augmentation through submission of a BCP or Budget Revision to increase the agency's existing information technology activities.
- The project is a new system development or acquisition made in response to a legislative mandate or the project is subject to special legislative review as specified in budget control language or other legislation.
- The project involves direct public access by private sector organizations or individuals to State data bases .
- The project involves contracts for professional, managerial, or technical services (excluding services received through interagency agreements) totalling more than $25,000.
- The project involves acquisition of one or more personal computers, personal computer software, or related peripherals, and the agency does not have an approved Workroup Computing Policy (SAM Section 4989 et seq.).
- The project involves installation or expansion of wide area network data communication services other than those offered by the DGS, Division of Telecommunications, or a State consolidated data center as defined in SAM Section 4982.
- The project involves one or more of the following emerging technologies and more than $25,000 will be spent on acquisition of hardware or software required for the technology:
  - Document imaging.
  - Geographic information systems.
  - Computer aided systems engineering.
  - Expert systems/artificial intelligence.

43020.4.4.2 Cost Thresholds

Cost thresholds are assigned to agencies based on their size and past experiences with information technology projects. CDC is a Category1agency; therefore any CDC project shall be a reportable project if it will cost more than $500,000.

43020.5 FSR

CDC adheres strictly to State policy requiring that a feasibility study be conducted and a FSR be approved prior to the expenditure of resources on any information technology project. The only exception to this requirement is the justification and acquisition of personal computers and related commodities through use of the Workgroup Computing Justification Form (SAM Section 4991.1).

The term Information Technology Project is defined in DOM 41010.3, EDP Definitions.

The feasibility study shall be performed in conformance with the requirements of SAM Sections 4922 through 4927.

The FSR shall be prepared in accordance with SAM Sections 4928 through 4928.4.

The FSR shall be reviewed and approved in accordance with the general requirement of SAM Section 4819.3, State Information Management Authority and Responsibility, as well as the specific requirements of SAM Sections 4926 through 4926.5.

Refer to SAM and the handbook, "How To Conduct A Feasibility Study," published by OIT, for specific guidelines for completing each step of the process.

43020.5.1 FSR Purpose

The Feasibility Study represents the first opportunity within the project management sequence for State management to assess the full implications of a proposed information technology project. The purposes of the Feasibility Study are to:

- Determine whether a proposed project represents a justified expenditure of public resources in terms of whether it:
  - Is responsive to a clearly defined, program-related problem or opportunity.
  - Is the best of the possible alternatives.
  - Is within the technical and managerial capabilities of the agency.
  - Would provide benefits over the life of the application that exceed development and operations costs. Such benefits typically include reduced program costs, avoidance of future program cost increases, increased program revenues, or provision of program services that can be provided only through the use of information technology.
- Provide a means for achieving agreement between agency executive management, program management, and project management as to:
  - The nature, benefits, schedule, and costs of proposed project.
  - Their respective management responsibilities over the course of the project.
- Provide executive branch control agencies and the Legislature with sufficient information to assess the merits of the proposed project and determine the nature and extent of project oversight requirements.

43020.5.2 Internal Approval Process

In addition to the State policy and procedures which govern information technology projects, FSRs shall be developed and approved according to the following internal process. Once the FSR and/or CDC internal Project Summary Fact Sheet is completed and approved by the Division approving authority, it is submitted to:

- ISD, Project Initiation Unit (PIU), for technical review and recommendation.
- MIS-SU for inclusion on MIS Committee agenda.
- MIS Committee for final departmental approval.
- ISD/PIU for submission to OIT for review and approval if the project is reportable.
- ISD/PIU for preparation of certification statement (Certifications for Personal Computer systems approved through the Personal Computer Policy are prepared by the MIS-SU).
- Chairperson, MIS Committee, to sign certification.
- Deputy Director, ASD, and Assistant Director, OOC, to sign certification.

OIT's response to the Department regarding project approval/disapproval is sent directly to the Chief Deputy Director and then to ISD. Subsequently, ISD shall update the project file and route copies to the project initiator(s) and to MIS-SU.

The process differs slightly if a BCP is required. In order to ensure that the FSR is developed and approved within the mandatory time frames, refer to DOM 43020.3.1.

In addition to a project file, ISD (Systems Support) also monitors initial and subsequent equipment procurements to ensure they fall within the scope of the approved FSR or CDC Internal Summary Fact Sheet. Copies of all approved procurement documents shall be routed to the MIS-SU.

43020.6 Revisions

The Assistant Director, OOC, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

43020.7 References

SAM §§ 4819.2, 4819.3, 4819.34, 4900, 4902.1, 4920, 4922 - 4928.4, 4989, 4991.1, and 6100.

OIT, Information Management Guidelines: How To Conduct A Feasibility Study.

DOM §§ 21010, 41020, 41010.3, 43010.1.1, 43020.3.1, 43020.3.2, 43020.4, 43020.5, and 48010.2.

ARTICLE 9 — PROJECT MANAGEMENT

Revised October 17, 1994

43030.1 Policy

It is the policy of the Department to create an automation organizational structure that is conducive to the successful implementation, maintenance, and control of the EDP environment.

43030.2 Purpose

The purpose of this policy is to ensure that an EDP infrastructure is created which meets the needs of the Department and fixes responsibility and authority for the development and maintenance of EDP systems.

43030.3 Responsibility

EDP project management is project team oriented. Maintenance and development projects each have a technical project manager. New development projects also have a user project manager. Each project, whether maintenance or new development, is uniquely and individually staffed with a separate project team. DOM 43030.4 describes the structure of project teams.

Team Concept

Project Team Structure

The project team is a self-sufficient unit staffed with the appropriate technical and managerial resources to address the complexity and size of a project through its

life cycle--from initiation through the development, implementation, and maintenance phases. A project team shall have the following composition:

- A core technical staff of analysts and programmers to construct the system.
- Users to participate in requirements definition, design "walkthroughs," and test planning and execution.
- Trainers to develop user manuals and to train users.
- Administrative staff to support project tracking and management reporting.

Each project shall have a technical project manager and an associated user group. New development projects shall also have a user project manager who shall stay with the project through implementation. The user project manager shall be responsible for "what" needs to be automated. The technical project manager shall be responsible for the technical aspects (i.e., the "how") of the project. DOM 43030.5 (User Project Manager) and DOM 43030.6 (Technical Project Manager) outline the roles and responsibilities of the user and technical project managers, respectively.

User Project Manager

The user project manager is selected by CDC executive management from one of the functional areas affected by the project and reports to the appropriate Deputy Director on the MIS Committee.

The user project manager provides overall guidance to the technical project manager. The user project manager keeps fully apprised of the status of the project through regular written project reports from the technical project manager, although the technical project manager reports formally to ISD management.

The user project manager is fully responsible for the project and, in effect, is subcontracting for technical expertise. Therefore, this contract is with ISD rather than a specific technical project manager. This means that the usual reporting structure for ISD is maintained.

The user project manager is responsible for securing the necessary project funding and project resources. In addition, the user project manager is responsible for ensuring that the IMAP, BCS, BCP, FSR, Special Project Report (SPR), Quarterly Project Report (QPR), Post implementation Evaluation Report (PIER), and any other required documentation is prepared and approved by departmental management. ISD shall be responsible to review, log, and submit these reports to EDP control agencies as required.

The user project manager communicates project needs and priorities to the technical project manager, as reported by the user group. The user project manager is also responsible for ensuring that the user community provides the necessary time and resources required throughout the project, such as needs and requirements analysis, data conversion, and user training, as addressed in the approved project management plan.

Technical Project Manager

The technical project manager is appointed by ISD and reports to a unit manager within the Applications Systems Section who, in turn, reports to the ISD Application Systems Manager. The technical project team members report directly to the technical project manager.

The technical project manager has full authority over and responsibility for the technical aspects of the project and the technical project team members. This responsibility includes:

- Detailed planning.
- Staff recruitment and management.
- Project budget control.
- Requirements specifications.
- System design.
- Programming and testing.
- System implementation.
- Data file conversion (responsibility for this task shall be shared with user staff depending upon the resources allocated to the project and the conversion approach approved in the implementation plan).
- System maintenance.
- User training (responsibility for this task may vary depending upon the resources allocated to the project and the training approach approved in the project management plan).

User Groups

Each project (whether new development or maintenance) shall establish an associated user group comprised of representatives from the user community. The purpose of these user groups is to provide a forum for communication between the project teams and those who use the application systems, in order to facilitate more effective use of existing application systems and assist in the development of new systems.

The user group representatives prioritize requests for system enhancements, exchange information on system usage, and provide feedback on system modifications.

43030.4 Revisions

The Assistant Director, OOC, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

43030.5 References

DOM §§ 43030.4 - 43030.6.

ARTICLE 10 — PROJECT REVIEW AND BASIC POLICY

Revised October 17, 1994

44010.1 Policy

The Department has established policy regarding project reporting and evaluation for each approved information technology project, in accordance with the requirements of SAM 4940 of the. All operating units within CDC shall adhere to the requirements set forth in the current section concerning project review, reporting, and evaluation. Additional requirements may be specified by the Office of Information Technology (OIT) in response to the Department's IMAP or in response to other needs reported by the Department (agency requirements are provided in SAM 4819.3 through 4819.39).

44010.2 Purpose

The purpose of this policy is to ensure that State and CDC project review requirements are implemented on an ongoing basis.

44010.3 Project Review Overview

Once the FSR for an information technology project has been approved by the MIS Committee (also by OIT for non-delegated projects or the DGS for projects involving communications), the design, acquisition, development, and implementation phases of the project may proceed.

The success of each phase of the project shall be evaluated and reported in terms of the project objectives. Included are project reports, a formal management review, and a post-implementation assessment. (SAM 4944 through 4946.2 provide a framework for project monitoring and evaluation.)

44010.3.1 Information Technology Project Reports

Two information technology project reports are specified, the Quarterly Project Report (QPR) and the Special Project Report (SPR). These reports:

- Support continuing communication among all project participants (project management, program management and executive management).
- Expose potential problems with respect to the availability of resources or the meeting of mandated project dates.
- Provide for CDC management and control agency review of project progress at appropriate intervals throughout the life of the project.

44010.3.2 Formal Project Review

In addition to the QPR and SPR, a major management briefing, known as the Formal Project Review (FPR) may be initiated by CDC management or required by the OIT for any information technology project. The FPR allows for CDC management or control agency review of large projects after completion of the general design phase, but before substantial resources have been committed to the project. It may also be employed to provide a formal management assessment of a project at any point during the development cycle.

44010.3.3 Post Implementation Assessment

Following completion of each information technology project, CDC shall carry out a post-implementation assessment. The assessment shall:

- Measure the benefits and costs of the newly-implemented information technology application or system against the original objectives.
- Document projected operations and maintenance costs over the life of the application or system.

44010.3.4 EDP Audit

Every two years the Department shall carry out and submit to the DOF an EDP audit. This audit is the responsibility of the Internal Audit Unit of PFAB (see DOM 49040). The audit shall be consistent with the DOF publication,

"Information Technology Security and Risk Management Guidelines." This guide reflects the SAM requirements regarding the responsibility and control of EDP policy, and provides audit guidelines; however, it may not cover all areas to be audited. The guide and information about it are available through the Internal Audit Unit of PFAB.

To accomplish this audit it is likely that ITS under development shall be selected for audit on a sample basis. The intent of the audit is to make an assessment of the degree of compliance by CDC with departmental and State policies and procedures. The scope of the audit shall include, but not be limited to, the following:

- Project approvals, feasibility study, and risk analysis (DOM 49020).
- Operational recovery plan (DOM 49030).
- Information security practices.

The Project Manager is responsible for ensuring that the project documentation is in compliance with policy.

44010.4 Project Review Central Control/Clearinghouse

All IMAP "external" and "internal" reporting activities shall be monitored by CDC management through a central control agency/contact with regard to OIT reportable projects, OIT projects delegated to the Department, and all other Department information technology projects with an approved FSR, including those requiring a Summary Fact Sheet or Workgroup Computing Justification Form. The ISD, System Support Unit (ISD-SSU) shall be responsible for the central clearinghouse function. Refer to DOM 43030.3, User Project Manager, for project reporting responsibilities.

Responsibilities

The ISD-SSU central clearinghouse monitors all external and internal quarterly project reports, special project reports, and post-implementation assessments. Project managers shall ensure that appropriate sign-off is attained on all projects before documents are submitted to the central clearinghouse. It is the responsibility of the central clearinghouse to:

- Develop a cataloging system to monitor the completion and distribution of required reporting per schedule.
- Notify project managers of scheduled reports prior to the report due date.
- Review completed reports to ensure adherence to the State-required format.
- Maintain copies of all reports and, in effect, act as a liaison between OIT and CDC project management concerning reporting requirements throughout the life cycle of the project.

Summary Information Report

Since ITS approval and oversight are the responsibility of the MIS Committee, the central clearinghouse function shall provide summary information on each ITS project to the MIS Staff Committee at its quarterly meetings. This summary information shall include:

- The project title.
- MIS approval date.
- Projected completion date.
- OIT delegation status.
- FSR status.
- QPR status.
- PIER status.

The central clearinghouse shall also provide the MIS Committee with a summary project status profile which may be in the form of the project's most current QPR and, if necessary, SPR.

44010.5 Project Compliance Review

The Department is subject to compliance reviews conducted by OIT, or by specified units within CDC. The purpose of a compliance review is to verify CDC adherence to Department and State information technology policies and procedures.

Types of Compliance Reviews

ITS within CDC are subject to four types of reviews:

- Type 1. Policy compliance reviews (SAM Section 4942).
- Type 2. EDP audit reviews (see DOM 49050).
- Type 3. Information security, risk management, operational recovery compliance reviews (SAM Sections 4840 through 4845; DOM 49000).
- Type 4. Facility peer reviews.

Policy Compliance Review

Type 1 - Policy compliance reviews are conducted by OIT. Responses to this type of review shall be coordinated by the central clearinghouse function of ISD.

EDP Audit Reviews

Type 2 - EDP audit reviews are part of an audit required by SAM, and are usually conducted by the Internal Audits Unit of PFAB. Alternately, it is possible that Type 2 reviews shall be carried out by the Audits Group of DOF, but responsibility for the audit reviews remains with PFAB. The owner of an information system is responsible for providing responses to audit findings regarding that system.

Security, Risk, and Operational Compliance Reviews

Type 3 - Information security, risk management, and operational recovery compliance reviews are ongoing and conducted by the Information Security Unit within PFAB. These reviews are usually not oriented to a specific system or project, and are limited in scope to the policies contained in SAM Sections 4840 through 4845, and DOM Subchapter 49000.

Facility Peer Reviews

Type 4 - Facility peer reviews are reviews of business services operations conducted by the Department on a rotational basis at each of CDC's facilities. The EDP portion of the peer review includes a functional review of Offender Based Information Services, the DDPS, and personal computer security practices and system utilization.

The review teams are composed of business services and administrative staff from headquarters and the facilities.

NonDelegated Projects

OIT reviews project reporting documentation in conjunction with its compliance review and oversight responsibilities.

Delegated Projects

For delegated projects, the MIS Committee shall determine when a compliance review is to be conducted, the scope of the review, and who shall perform the review.

44010.6 Revisions

The Assistant Director, OOC, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

44010.7 References

SAM §§ 4819.3 to 4819.39, 4840 - 4845, 4940, 4942, and 4944 - 4946.2.

DOM §§ 49000, 49020, 49030, 49040, 49050, 43030.5.

DOF publication, "Information Technology Security and Risk Management Guidelines."

ARTICLE 11 — PROJECT REPORTING REQUIREMENTS

Revised October 17, 1994

44020.1 Policy

It is the policy of the Department to monitor the implementation and outcome of EDP projects within the Department to ensure that progress and outcome information is tracked and reported, as specified by SAM 4940 and as otherwise required by State oversight agencies. Additional requirements may be specified by the Office of Information Technology (OIT) in response to the Department's Information Management Annual Plan (IMAP) or in response to other needs reported by the Department (see SAM 4819.3 through 4819.39 for departmental requirements).

44020.2 Purpose

The purpose of this policy is to ensure that adherence to all project reporting requirements outlined by State oversight agencies is monitored and met.

44020.3 Project Reporting Requirements– Compliance Review Reporting Schedule

The Compliance Review Reporting Schedule for both delegated and non-delegated projects is set by the MIS Committee in accordance with central control agency and Department requirements, and is reported to the central clearinghouse.

44020.4 Project Reporting Requirements—Audit of Information Technology Projects

All information technology projects are subject to audit, with project reporting and evaluation documents being an essential aspect of the audit trail (SAM Section 4943). CDC is subject to project audits by control agencies as well as internal audits. Documentation supporting project decisions shall be kept by the

Department in the central clearinghouse for a minimum period of two years following approval of the post-implementation assessment.

Nondelegated Projects

OIT audits project reporting documentation in conjunction with its audit and oversight responsibilities.

Delegated Projects

For delegated projects, the MIS Committee shall determine when an audit is to be conducted, the scope of the audit, and who shall perform the audit.

44020.5 Project Reporting Requirements– Project Audit Reporting Schedule

The project audit reporting schedule for both delegated and non-delegated projects is set by the MIS Committee in accordance with central control agency and Department requirements, and is reported to the central clearinghouse.

44020.6 Project Reporting Requirements– Quarterly Project Report Requirements

Quarterly Project Reports (QPR) are usually required of the project manager in the case of projects subject to monitoring by OIT, and may be required as an additional reporting responsibility for delegated projects. OIT's response to the Department's IMAP or FSR specifies the necessity of preparing QPRs for particular projects. On occasion, reporting on other than a quarterly basis is established by the FSR and approved by the MIS Committee.

Every external QPR shall be reviewed and approved by the affected division, and by the Director, or designee. Two copies of the QPR shall be submitted to the central clearinghouse for submittal to OIT by no later than the 15th day of the month following the end of each fiscal quarter (i.e., October 15, January 15, April 15, and July 15). A copy of the QPR shall be forwarded to the Office of the Legislative Analyst.

CDC also encourages use of the QPR format to document project activity for projects that do not qualify as reportable, or for which project monitoring has been delegated to the Department. These internal QPRs shall be reviewed and approved by the affected division. It is not necessary to forward copies of these reports to OIT or the Office of the Legislative Analyst unless so required by OIT.

The QPR shall contain a brief summary of project status including an explanation of any minor deviations from the original project plan. An updated Project Management Schedule (see SAM Section 4928.4) showing actual completion dates of specific tasks/deliverables shall be attached. The QPR shall conform to the standard format provided in SAM Section 4944.1.

Some deviations from the project plan require preparation and submission of a Special Project Report (SPR). The conditions that require preparation of an SPR are defined in SAM Sections 4945 and 4945.1.

44020.7 Project Reporting Requirements– Special Project Reports

General Reporting Requirements (SAM Section 4945): Preparation of an SPR is required whenever a project deviates substantially from the costs, benefits or schedules documented in the approved FSR, or when a major revision occurs in project requirements or methodology. No expenditure of funds shall be made to implement an alternative course of action until approval has been received from OIT or the Director of CDC, as appropriate (SAM Section 4945). SAM Section 4945.1 lists specific conditions for the required submission of an SPR to OIT.

SPRs, which must be submitted to OIT, shall be transmitted within 30days after recognition of a substantial deviation. Two copies of the SPR shall be submitted to OIT and one copy to the Office of the Legislative Analyst. SPRs shall be signed by the Director of CDC or designee.

If a QPR is due to OIT during the period the Department is engaged in preparing the SPR, CDC shall submit the QPR (see SAM Sections 4944 through 4944.1) stating that an SPR is under development and providing an approximate date for its completion.

The format and content of the SPR transmittal letter for each non-delegated or delegated project shall conform to the standard formats provided in SAM Section 4945.

Conditions Requiring Submission to OIT (SAM Section 4945.1):

- Projects subject to OIT approval/oversight - an SPR shall be submitted to OIT if:
  - The information technology project's total costs deviate p roj, or are anticipated to deviate, by ten percent (higher or lower) from the estimated information technology ect budget (to be measured against the combined total of each fiscal year's One-time Costs plus Continuing Costs on the Summary Fact Sheet, SAM 4930 Illustration 1.
  - The project schedule falls behind or is anticipated to fall behind by 10 percent or more (to be measured using the key management milestones critical to project success reported on the Summary Fact Sheet, SAM Section 4930, Illustration1).
  - The total program benefits deviate or are anticipated to deviate by 10 percent (higher or lower) from the estimated total program benefits (to be measured against the combined total of each fiscal year's Cost Savings and Cost Avoidances on the Summary Fact Sheet, SAM 4930, Illustration 1).
  - A major change occurs in project requirements or methodology.
- Projects subject to approval and oversight by the Special Project Director (delegated or nonreportable), and projects for which project reporting has been delegated to the Director afterOITapproval of the FSR: Submission of an SPR to OIT is required if the revised project costs exceed or are estimated to exceed CDC's IMAP cost threshold (SAM Section 4902.12), and one or more of the following conditions are true:
  - The total information technology project costs deviate or are anticipated to deviate by 10 percent (higher or lower) from the estimated information technology project budget (to be measured against the combined total of each fiscal year's One-time Costs vs. Continuing Costs on the Summary Fact Sheet, SAM Section 4930 Illustration 1).
  - The project schedule falls behind or is anticipated to fall behind by 10 percent or more (to be measured using the key management milestones critical to project success reported on the Summary Fact Sheet, SAM 4930, Illustration 1).
  - The total program benefits deviate or are anticipated to deviate by 10 percent (higher or lower) from the estimated total program benefits (to be measured against the combined total of each fiscal year's Cost Savings and CostAvoidances on the Summary Fact Sheet, SAM Section 4930, Illustration 1.
  - A major change occurs in project requirements or methodology.
- If an SPR for a delegated project must be submitted to OIT, attach to the SPR a copy of the approved FSR and the project approval letter signed by the Director or designee.
- Internal special project reports–Delegated or nonreportable projects which exceed projected project development costs but do not (according to control agency requirements) require an SPR.

An internal SPR shall be required when the cost thresholds below are exceeded:

- By less than $100,000–The project exceeds cost projections by 25 percent or more.
- Between $100,000 and $200,000–The project exceeds costs projections by 15 percent or more.
- Over $200,000–The project exceeds cost projections by 10 percent or more.

The SPR shall provide sufficient information for Department management, executive branch control agencies, and the Legislature to assess the merits of the proposed project change and determine the nature and extent of future project oversight requirements. If an SPR lacks sufficient information for these purposes, OIT may request that the Department provide additional information.

SPRs shall be commensurate with the level of deviation from the approved FSR. Therefore, the Department shall determine whether to prepare a revised FSR, provide the information required by the minimum content for an SPR (defined below), or do something in between these two extremes.

The minimum content for an SPR consists of a description of the project status, an explanation of the reason for the project deviation, a revised project management schedule, and economic summary information. CDC shall prepare an SPR with at least the minimum content described below:

- Project Status - An explanation of the problems encountered or opportunities identified that have led to the preparation of the SPR. This section of the SPR shall include as appropriate:
  - Changes in Project Requirements or Methodology - An explanation of the proposed change from the anticipated course of action, including the reasons for the change and why this proposed alternative methodology is now the preferred course of action.

- Cost Benefit or Schedule Deviations - An explanation of the deviation from the originally anticipated costs, benefits or schedule. This section shall include the reasons for the deviation and the proposed course of action to bring the project back within planned costs, benefits, or schedule.

- Summary Fact Sheet - This section shall include a revised Summary Fact Sheet (SAM Sections 4930 through 4930.1) indicating accomplishments to date by using actual dates in the Target Date fields of the Project Schedule, then continuing the schedule by focusing on the yet to be accomplished milestones critical to project success. The cost analysis portion shall contain all actual costs to date plus revised projected costs through the end of the project.

For example, this may be the second fiscal year that the project has been under development: indicate the actual project costs for last year and place them in the first column of Personnel Years (PYs) and Costs, then combine the actual costs for the current fiscal year-to-date with the anticipated costs for the remainder of this fiscal year, and place them in the second column of PYs and Costs. Indicate the anticipated costs for each succeeding budget year through the end of the project.

If the feasibility of the project was documented through the preparation of a FSR, the following additional content shall be provided:

- Project Management Schedule - A revised Project Management Schedule (SAM Section 4928.4) indicating accomplishments to date and focusing on the duration of critical tasks, major management decision-points, and progress reporting milestones shall be included in the SPR.

- Economic Analysis Worksheet - A revised Economic Analysis Worksheet (SAM Sections 4929 through 4929.2) shall be provided. The worksheet shall contain all actual costs to date plus revised projected costs through the end of the project.

For example, this may be the second fiscal year that the project has been under development: Indicate the actual project costs for last year and place them in the first column of PYs and Costs, then combine the actual costs for the current fiscal year-to-date with the anticipated costs for the remainder of this fiscal year, and place them in the second column of PYs and Costs. Indicate the anticipated costs for each succeeding budget year through the end of the project.

44020.8 Project Reporting Requirements-- Formal Project Review

A Formal Project Review (FPR) may be initiated by Department management or required by OIT for any information technology project. The FPR typically provides a formal management or control agency checkpoint after completion of the project's general design phase, but before substantial resources have been committed. It may also provide a formal management assessment of a project at any point during the development cycle. (FPRs may be scheduled during the procurement process if doing so does not violate procurement requirements.)

OIT may notify the Department that an FPR is required in its response to the Department's IMAP, in an FSR approval document, or in any correspondence subsequent to project approval.

SAM Section 4946.1 provides guidance in the form of recommended content for the preparation and presentation of an FPR. Depending upon the complexity, sensitivity, and size of the project, an FPR presentation shall usually require between two and four hours. When the Department receives services from a data center or from another agency, responsible staff should request that representatives of the data center or the servicing agency attend.

Content and Organization

The FPR provides an opportunity for a final critique of the merits of the proposed information technology project prior to commitment of substantial resources. It shall be used also as a checkpoint during project development to maintain management involvement and awareness with respect to crucial decision points. The FPR allows assessment of: (1) systems design, (2) current estimates of costs and benefits, (3) management controls, and (4) probability of project success.

Composition of Formal Project Reviews (FPR)

An FPR topic outline is provided in SAM Section 4946.1, Illustration 1. Typically, the FPR is organized into four major sections:

- Background.
- Technical Strategy.
- Project Management Controls.
- Summary.

The suggested content of each of these sections is specified in SAM Sections 4946.11 through 4946.14.

It is important to adapt the presentation to suit the audience. Executive management, for example, may not be interested in the technical details of a project, but may be anxious to know the time frames for system operation and the capture of proposed tangible and intangible benefits.

Background Section

The Background Section of the FPR shall provide the facts necessary to understand the problem or opportunity being addressed by the project, and the defined project objectives within their program context.

Typically, this portion of the presentation shall include:

- A summary of the information contained in the requirements section of the FSR, with a note of any significant changes since preparation of the FSR.
- A brief overview of the project technical strategy as defined in the FSR's functional requirements (technical topics are normally covered in detail during the technical strategy section of the FPR).
- A brief description of project organization as it relates to the overall organization of the Department, and any specific user organization within the Department.
- An overview of the information contained in the Management Plan Section of the FSR.
- A management summary that concentrates on costs, benefits, savings, PY reductions, or other quantifiable or non-quantifiable management benefits that were described in the FSR.
- A synopsis of anticipated decisions that shall be necessary at the conclusion of the presentation.

Ideally, the FPR is based upon information that is more current than is contained in the FSR; therefore, the estimates should be an update to the economic analysis portions of the FSR.

The presentation on technical strategy shall include typically:

- Major system processes, including file or data section base relationships, interfaces with existing systems, and impact on other systems currently in operation, planned, or under development. This overview of systems capabilities should inform the audience regarding methods for processing information, input mechanisms, output mechanisms, error detection techniques, and data distribution or access.
- Specific hardware and software requirements for development and operation of the system; the level of presentation detail should be based on the audience's technical background and need to make informed decisions.
- Lease versus purchase decisions for equipment and software, and the procurement mechanism and schedule.
- Requirements for security and asset protection: level of security, security methods, and contingency plans.

Project Management

This section provides an overview of the project management plan based upon the Management Plan section of the FSR with updates to reflect changes since the preparation of the FSR. Additionally, a review of the project phases is typically presented including design, development, testing, implementation, conversion, and acceptance. Coordination of responsibility for these phases is also presented.

Other topics included in the project management section of the presentation are:

- Training requirements, plans, and costs for technical and user staff.
- Special management requirements for system conversion.
- User or technical responsibilities for data conversion.
- The time frame for accomplishment of conversion.

Summary

The concluding section of the FPR normally summarizes the current status of the project, describes the next steps in the project, highlights potential problems for the project, and closes with any required decisions that may be necessary.

44020.9 Revisions

The Assistant Director, OOC, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

44020.10 References

SAM §§ 4819.3 - 4819.39, 4902.12, 4928.4, 4929 to 4929.2, 4930 to 4930.1, 4940, 4943, 4944 to 4944.1, 4945 to 4945.1, 4946.1, and 4946.11 - 4946.14.

ARTICLE 12 — PROJECT EVALUATION

Revised October 17, 1994

44030.1 Policy

It is the policy of the Department to evaluate its EDP projects as required by the SAM 4940, and as otherwise required by State oversight agencies. Additional requirements may be specified by the Office of Information Technology (OIT) in response to the Department's Information Management Annual Plan (IMAP) or in response to other needs reported by the Department.

44030.2 Purpose

The purpose of this policy is to ensure the implementation of all project evaluation requirements specified by laws and regulations, and State and departmental policies.

44030.3 Post-implementation Evaluation Report (PIER) General Information

A post-implementation assessment shall be carried out by the Department following the completion of each information technology project. No project is considered complete until the report of that assessment, the Post-implementation Evaluation Report (PIER), has been approved by OIT or the Department Director, as specified in OIT's response to the Department's IMAP and in accordance with SAM 4819.36 and 4941. Approval of a PIER by OIT or The Director, as required, terminates project reporting requirements.

The post-implementation assessment shall be conducted after the new information technology capability has been operational for a sufficient period of time to allow its benefits and costs to be accurately assessed. Initial operational problems shall have been resolved and sufficient experience and data shall have been accumulated to determine whether the project met the proposed objectives, was completed within the anticipated time and budgetary constraints, and achieved the proposed benefits. The optimum time after implementation to conduct the assessment depends upon the nature of the project. Six months after implementation is typical. The assessment shall be completed within two years of implementation of the information technology capability.

The required content for a PIER is defined in SAM Section 4947.2. The format and content of the PIER Transmittal Letter for each non-delegated project shall conform to the standard format shown in SAM 4947, Illustration 1. The format and content of the Transmittal Letter for each delegated project requiring submission of the PIER to OIT shall conform to the standard format shown in SAM 4947, Illustration 2.

44030.4 PIER Reporting Requirements

Two copies of the PIER shall be submitted to OIT and one copy to the Office of the Legislative Analyst if the project was subject to approval and oversight by OIT. If OIT has delegated project approval authority to CDC, but in conjunction with that delegation has required that CDC submit a copy of the PIER following completion of the project, CDC's submission of the PIER shall include a copy of the approved FSR with its signed Project Approval Letter.

PIERs for projects subject to approval and oversight by the Department Director (delegated or non-reportable) or projects for which project reporting has been delegated to the Department Director after OIT approval of the FSR shall be approved by the Director or designee (see SAM 4971.1).

44030.5 PIER Content and Format

The level of detail included in the PIER shall be commensurate with the scope and complexity of the project and its anticipated benefits. The narrative portion of the PIER for a minor project can be as brief as one or two pages. However, it shall provide sufficient information for Department management, executive branch control agencies, and the Legislature to assess the success of the project (see SAM Section 4947.2).

PIER Composition

The PIER is comprised of five sections:

- Background and Summary of Results Section. A brief summary is provided of the project history, objectives, and results. Topics to be discussed normally include: how the project was initiated, how it progressed, problems that were overcome, user and management acceptance of the operational application, how Department management views the management of the project, and how the application fits into the Department's overall management and operations strategy.
- Attainment of Objectives Section. Specific objectives are established during the feasibility study for each project and are documented in the FSR. These objectives, which are normally defined in terms of measurable impact on Department programs and resources, provide the baseline for measurement of the project's success. Accordingly, the narrative portion of this section of the PIER shall describe the project outcome with respect to each objective included in the FSR. This section shall also include a clear statement regarding the capture of benefits and whether they were achieved as anticipated.

Two attachments shall be included with this section of the PIER:

- Attachment 1--PIER Economic Summary Report. Project costs and benefits shall be summarized using the PIER Economic Summary (SAM 4947.2 Illustration1). This spreadsheet allows comparison of the anticipated costs of the selected alternative, as documented in the FSR Economic Analysis Summary (SAM 4929.3), with actual project costs from the project start date through the period of project operation chosen as the basis for the PIER. For detailed information on the completion of entries in the PIEREconomic Summary, see the instructions for the FSREconomic Analysis Worksheet (SAM 4929.1 through 4929.2) and the Economic Analysis Summary (SAM 4929.3).
- Significant deviations from the anticipated costs shall be explained in the narrative portion of this section.
- Attachment 2–Project Management Schedule Report. Arevised Project Management Schedule (see SAM 4928.4) showing targeted and actual completion dates for major accomplishments during the project shall be provided, with significant deviations from the original schedule explained in the narrative.
- Projected Operations/Maintenance Costs Section. The Summary of Projected Operations/Maintenance Costs documents anticipated costs of systems operation and maintenance by fiscal year over the expected operational life of the application or system. These costs shall begin where the costs contained in the PIER Economic Summary ended. For detailed information on completion of the specific line items in the Summary of Projected Operations/Maintenance Costs, see the instructions for continuing costs found on lines 9-16 of the FSR Economic Analysis Worksheet contained in SAM 4929.1 through 4929.2.
- Special Observations Section. This section is optional. If completed, it should contain a narrative of any notable occurrences or factors that contributed to the project's success, or problems or other information that could be helpful during future project efforts.
- Corrective Actions Section. This section shall be included when the project is deemed to be a limited success or a failure, or when there are significant differences between project expectations (as expressed in the FSR) and project results.
  - If the project was a limited success or involved significant differences between expectations and results, alternatives for improving the outcome shall be summarized. If the project was a failure, available alternatives for addressing the problem or opportunity shall be summarized.

44030.6 Revisions

The Assistant Director, OOC, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

44030.7 References

SAM §§ 4819.36, 4928.4, 4929.1 - 4929.3, 4941, 4941, 4941.1, and 4947 - 4947.1.

ARTICLE 13 — POLICY AND GENERAL INFORMATION

Revised October 19, 1994

45010.1 Policy

The Department shall require competitive acquisition of EDP goods and services in accordance with applicable provisions of the SAM, the PCC, the GC, and the LC.

45010.2 Purpose

This section describes the departmental requirements for procurement and contract of EDP goods and services.

45010.3 EDP

EDP is referred to as information technology, encompassing all computerized and auxiliary automated information handling including systems analysis and design, conversion of data, computer programming, information storage and retrieval,

voice/video aspects, requisite system controls, data communications, simulation, and all related interactions between people and machines.

45010.4 Responsibility

Contract Services Section

The Department's Contract Services Section (CSS) shall supervise EDP contracts entered into by CDC in a manner that:

- Conserves the financial interests of the Department and the State.
- Prevents, so far as possible, any thriftless acts by employees of CDC.
- Avoids unnecessary expenditures.

BSS

The BSS is responsible for the preparation of purchase documents for all EDP equipment and data-related items for use in CDC headquarters or by the P&CSD. As directed by the Department, the BSS is responsible also for the procurement of EDP equipment by specific facilities.

- BSS shall ensure that all requests submitted for purchase are complete and the necessary documentation is included, such as certifications or FSRs.
- BSS is the departmental contact with the DGS, Office of Procurement, for all EDP procurements processed for CDC headquarters and P&CSD, as well as for specified facility procurements.

P&CD

The P&CD is responsible for procurement of EDP equipment for new prison construction projects.

DGS

The DGS is the State agency that exercises supervision over EDP contracts entered into by all other State agencies.

The DOF and DGS have general powers of supervision over matters concerning the financial and business policies of the State, and they are empowered to institute investigations and procedures deemed proper in the best interests of the State.

While most types of contracts are reviewed and approved by the Legal Services Division of DGS, EDP contracts are reviewed and approved by the DGS, EDP Acquisitions Unit. This unit reviews contracts to ensure that the best interests of the State are preserved, that State agencies comply with applicable laws, rules, and regulations, and that expenditures are made as wisely and economically as possible given the needs of agencies.

45010.5 Procurement/Contracting Project Authorization

Before a contract or purchase order for a new EDP project can be let for the purchase of goods and services, the program concept and any needed equipment and services shall be evaluated by the Department's MIS Committee. Also, the program concept and any equipment/services shall be contained in the Department's Information Management Annual Plan (IMAP) filed with DOF (see DOM 43010, Information Management Planning, for additional information). If accepted for incorporation in the IMAP, a feasibility study is conducted to thoroughly evaluate the concept and analyze the cost/benefits. The completed FSR shall be approved at all appropriate levels of Department management, and by the Director.

The FSR shall then be forwarded to the DOF, Office of Information Technology (OIT) for review and approval, unless the project is delegated to the Department (refer to DOM 43020, FSR Policy, for additional information). If approved, a budget concept paper may be prepared or a BCP initiated for review and approval by top management of the Department and DOF. Approval of the Legislature and the Governor also may be required through the budget enactment process. If the project is authorized, the drafting of contracts shall be initiated.

45010.6 Certification Affidavit for an EDP Purchase Order/Contract

Certain EDP purchase orders and contracts must be accompanied by a "Certification of Compliance with Policies Pursuant to SAM 4819.39 and 4832," as specified in SAM 4819.39 and 4832. Procurements not requiring such certification are:

- Procurements for less than $10,000;
- Procurements limited to only maintenance services;
- Procurements in support of previously approved efforts (see SAM 4819.38);
- Procurements of services to conduct a feasibility study provided the services are limited to supporting or conducting the feasibility study and/or preparing the FSR; or
- Procurements of/for excluded activities as described in SAM 4819.32.

The certification attests that the program or function for which the purchase documents are being processed has been approved by the DOF. SAM 4832 provides a sample of the certification affidavit.

In order to comply with the certification requirement, all EDP contracts and purchase orders not included by the above criteria shall be forwarded to headquarters. Additionally, every amendment to such EDP contracts or interagency agreements shall include a certification affidavit.

Certifications for microcomputers, peripheral equipment and software shall be prepared by MIS-SU. Certification for all other EDP equipment shall be prepared by the ISD. The certification shall contain a statement signed by the Director, or designee affirming that the equipment is in compliance with SAM-requirements concerning information technology. In CDC, the Director has delegated approval authority to the Deputy Director, ASD, and the Assistant Director, OOC. Adherence to this certification requirement adds approximately two weeks to the routing process within CDC headquarters.

45010.7 Revisions

The Deputy Director, ASD, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

45010.8 References

SAM §§ 4800, 4819.39, and 4832.

DOM §§ 43010 and 43020.

ARTICLE 14 — METHODS OF PROCUREMENT

Revised October 19, 1994

45020.1 Policy

The Department shall utilize acceptable methods of procurement when purchasing or contracting for EDP goods and services.

45020.2 Purpose

This section describes the acceptable methods of procurement and provides a reference for more detailed information and procedures.

45020.3 Process for the Procurement of EDP Goods/Services

The process for procurement of EDP goods and services is more complicated than for procurement of non-EDP goods and services. There is no single competitive procedure best suited universally for all categories of acquisition. Each procurement consists of differing elements that, overall, lend themselves more appropriately to one technique than to another. It is the statutory responsibility of the DGS to select the method of procurement to be used for each situation.

45020.4 Competitive Methods of Procurement

Basically, there are three methods of competitive procurement:

- Invitation for Bids (IFB).
- Request for Proposals (RFP).
- Request for Quotations (RFQ).

45020.4.1 Invitation for Bids

The IFB is highly structured and details the requirements in technical terms. Bids shall address specifically the requirements and technical specifications in order to be deemed a responsive bid.

45020.4.2 Request for Proposals

A RFP states the requirements in more general terms than the IFB. This method allows vendors to submit their own individualized proposals free of any precise State-imposed mix of hardware, software, etc.

45020.4.3 Request for Quotations

RFQs are used when EDP procurements are so straightforward and clearly defined that they do not warrant the time investment required to prepare and execute an IFB or RFP.

45020.5 Specific Procedures for Competitive Bid Process

Detailed information on the competitive bid process, including sample bid formats, is contained in SAM 5211 through 5222. Additionally, the competitive bid process followed by CDC is outlined in DOM 22040.23.

45020.6 Revisions

The Deputy Director, ASD, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

45020.7 References

SAM §§ 5211 - 5222.

DOM § 22040.23.

ARTICLE 15 — LEASE OF EDP EQUIPMENT

Revised October 19, 1994

45030.1 Policy

The Department shall process EDP equipment lease agreements in accordance with the requirements of SAM.

45030.2 Purpose

This section describes the equipment leasing requirements provided by applicable SAM sections.

45030.3 EDP Equipment Leasing-Agreements

Provisions governing the lease of EDP equipment are contained in SAM 5252 and in DOM 22040.26.8. SAM 5252 also contains a model EDP equipment lease contract to be used by all State agencies in developing a final contract for the lease of EDP equipment. SAM provisions allow CDC to tailor the model to conform with specific situations (see the illustration in SAM 5252 for additional information on the lease agreement).

Riders

The general terms and conditions normally contained in an EDP-equipment lease contract are set forth in the main body of the contract. Conditions and issues that are unique to the specific contract are set forth as "riders" to the contract.

45030.4 Leasing Initial EDP Computer Terminal Equipment

The initial complement of computer terminal equipment shall be leased or purchased. There are specific acquisition requirements for terminal equipment. Also, each system may have a unique procurement or leasing process. See DOM 47000, Departmental Systems, for specific information.

45030.5 Revisions

The Deputy Director, ASD, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

45030.6 References

SAM § 5252.

DOM § 47000

DOM § 22040.26.8.

ARTICLE 16 — PURCHASE OF EDP EQUIPMENT*

Revised October 19, 1994

Not Cleared For Statewide Use

45040. 1 Policy

The Department shall follow acceptable procurement practices and methods as defined in SAM and DOM.

45040.2 Purpose

This section describes the responsibility for initiating an EDP procurement and the methods used to purchase EDP equipment and software.

45040.3 Responsibility

The responsibility for initiating an EDP procurement is defined as follows:

Headquarters and the P&CSD

If the procurement request meets the criteria established by the Workgroup Computing Policy, the requesting unit shall be responsible for preparing the appropriate purchase documents including, but not limited to, a CDC Form 954, Intraoffice Requisition, and a Workgroup Computing Justification Form. The forms and any supporting documentation shall be submitted through the appropriate chain of command, as indicated on the forms, for approval prior to submission to MIS-SU, which in turn shall review the documents for completeness and consistency with the Department's information system standards. MIS-SU shall then route the forms to BSS at headquarters for procurement. See DOM 48010.2 for a definition of the Workgroup Computing Policy.

If the procurement request is not covered by the Workgroup Computing Policy, the requesting unit shall complete an FSR. The Project Initiation Unit located in ISD will provide assistance in completing FSRs.

Facilities

The requesting unit shall submit the request to the facility procurement office for approval and preparation of the required purchase documents. The facility shall forward the request to ISD for review and divisional approval. ISD shall then forward the request to the MIS-SU for further review and processing.

New Prison Construction/Capital Outlay

P&CD is responsible for submitting the documents to the MIS-SU for review, approval, and certification. P&CD shall prepare the appropriate purchase documents to acquire the EDP equipment.

45040.4 EDP Equipment Purchasing- Document Preparation

All purchase documents for procurement of EDP equipment for headquarters, P&CSD, and facility purchases that are funded at headquarters, shall be processed through BSS at headquarters.

Purchase documents for procurement of EDP equipment by capital outlay or by bond funds for new prison construction shall be processed through PCD.

45040.5 Methods For Purchasing EDP Equipment For Use Within The Department

EDP equipment can be purchased using a number of different methods. The methods are:

- Master Purchase Contract-Generally established by the DGS , Office of Procurement (refer to instructions on the contract for preparation and submission of required documents).
- State Price Schedule-Established by the DGS Office of Procurement (refer to instructions on the State Price Schedule for preparation and submission required documents).
- Delegated Purchasing Authority-Purchases may be made in accordance with the terms and conditions specified in the purchasing authority delegated by the DGS Office of Procurement.
- Purchase Estimates-These are for equipment that cannot be made through master purchase contracts, State price schedules, or delegated purchasing authority.

45040.6 Purchasing EDP Computer Terminal Equipment Within CDC

Computer terminal equipment shall be leased or purchased. There are specific acquisition requirements for terminal equipment. Each system may require a unique procurement or leasing process. See DOM 47000, Departmental Systems, for specific information.

45040.7 Revisions

The Deputy Director, ASD, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

45040.8 References

SAM §§ 3500 et seq., and 5000 et seq.

DOM § 47000.

DOM § 22030.

ARTICLE 17 — GENERAL CONTRACT REQUIREMENTS

Revised October 19, 1994

45050.1 Policy

The Department shall process EDP contracts in accordance with applicable requirements of SAM.

45050.2 Purpose

This section describes the General Contract Requirements provided in SAM.

45050.3 General Contract Requirements- Procedures

In general, contracts for EDP goods and services shall follow the same process and procedures used for all other contracts as outlined in SAM 1200 through 1269 and 5200 through 5293, and as contained in DOM 22040.

45050.4 General Contract Advertising Requirements in State Contracts Register

EDP contracts with a dollar value of $1,000 or more, with the exception of contracts for proprietary software, shall be advertised in the California State Contracts Register. The responsible program unit shall prepare a Standard Form 815, Request to Advertise in California State Register, or a Standard Form 821, Request for Exemption from Contract Advertising. The Standard Form 821 is used when time does not permit advertising due to a bona fide

emergency, or when the Department's best interest would be better served by a sole source vendor. The applicable form shall be forwarded to the DGS, EDP Acquisitions Unit, for processing and for approval of any exemption request.

45050.5 General Contracts Approval Authority

The DGS has delegated authority to all State departments to approve contracts of $12,500 or less. All EDP contracts exceeding $12,500 shall be forwarded for review and approval to the DGS, EDP Acquisitions Unit. A certification affidavit shall accompany every contract.

45050.6 Revisions

The Deputy Director, ASD, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

45050.7 References

SAM §§ 1200 - 1269, and 5200 - 5293.

DOM § 22040.

ARTICLE 18 — EDP MAINTENANCE CONTRACTS

Revised October 19, 1994

45060.1 Policy

The Department shall process EDP maintenance contracts in accordance with requirements of SAM and shall utilize the SAM model contract when developing EDP maintenance contracts.

45060.2 Purpose

The purpose of this section is to ensure that EDP maintenance contracts adhere to applicable SAM provisions.

45060.3 Maintenance Contracts for EDP and Telecommunications Equipment

SAM 5220 contains requirements pertaining to contracts for the maintenance of EDP and telecommunication equipment installed under State contracts. SAM 5255.11 and 5255.12 contain a model maintenance contract for use by all State agencies in developing a final maintenance contract for EDP equipment or software. The model contract shall be tailored by CDC to conform with each specific situation.

The CDC Contract Services Section (CSS) maintains an updated version of the SAM model contract. Contact CSS for the latest version available.

45060.4 Revisions

The Deputy Director, ASD, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

45060.5 References

SAM §§ 5220, 5255.11, and 5255.12.

DOM § 22040.

ARTICLE 19 — EDP PERSONAL SERVICES CONTRACTS

Revised October 19, 1994

45070.1 Policy

The Department shall enter into EDP personal services contracts in accordance with applicable provisions of SAM.

45070.2 Purpose

This section outlines the specific requirements necessary in contracting for EDP personal services.

45070.3 Contracts for EDP Personal Services

Contracts for EDP personal services shall be processed in accordance with SAM 1200 et seq., 5271, and 5272, and DOM 22040. In general, EDP personal services contracts are used for activities such as software package programming, and the development or design of program enhancements.

45070.4 Procedures for Obtaining Personal Services Contracts for EDP Equipment

When EDP personal services are needed CDC shall prepare a DGS, Office of Procurement (GSOP), GSOP Form 206, Master Service Agreement Order (MSAO). The request for personal services shall then be submitted to the DGS Data Processing Services Section (DPSS). This section maintains a pool of programmers to assist various State agencies. If there are no available staff within DPSS, the MSAO shall be forwarded directly to the EDP Acquisitions Unit within DGS. The EDP Acquisitions Unit will use their statewide master agreement to identify a contractor for the specified personal services. The approved MSAO shall then be returned to CDC. CDC shall contact the contractor to interview and select individuals employed by the contractor for the provision of needed services.

45070.5 Revisions

The Deputy Director, ASD, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

45070.6 References

SAM §§ 1200 et seq., 5271, and 5272.

DOM § 22040.

ARTICLE 20 — CONSULTING SERVICES CONTRACT

Revised October 19, 1994

45080.1 Policy

The Department shall enter into EDP Consulting Services contracts in accordance with applicable provisions of SAM.

45080.2 Purpose

This section outlines specific requirements to be followed in processing EDP consulting services contracts.

45080.3 Procedures for Obtaining Consulting Services Contracts

Contracts for EDP consulting services shall be processed in accordance with SAM 1200, 5222, and DOM 22040.26.10. These contracts are not to be confused with contracts for the provision of personal services. Specifically, consulting services contracts shall be advisory in nature, provide a recommended course of action, and have a tangible end product.

A certification affidavit is required for initial EDP consulting services contracts as well as for any amendments to such contracts. All contracts regardless of the dollar amounts involved shall be processed through CDC's Contracts Services Section.

45080.4 Revisions

The Deputy Director, ASD, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

45080.5 References

SAM §§ 1200 et seq., and 5222.6.

DOM § 22040.

ARTICLE 21 — INTER-AGENCY AGREEMENTS

Revised October 19, 1994

45090.1 Policy

The Department shall process interagency agreements for EDP services in accordance with applicable requirements of SAM.

45090.2 Purpose

This section provides information necessary for processing EDP interagency agreements.

45090.3 Procedures for Obtaining an Interagency Agreement

Interagency agreements for EDP services shall be let in accordance with SAM 1200 et seq., 5240, 8752, 8752.1, and 8758.1, and DOM 22040.29. Each agreement shall contain a clear understanding of the services or products to be provided, the responsibilities of each party, the basis for payments, and the period of performance.

A certification affidavit is required for all initial interagency agreements and for any amendments to existing agreements. Interagency agreements shall be processed through the Department's Contract Services Section.

Interagency agreements shall be developed on an STD Form 13. All interagency agreements in excess of $35,000 shall be submitted for approval to the DGS, EDP Acquisitions Unit.

45090.4 Revisions

The Deputy Director, ASD, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

45090.5 References

SAM §§ 1200 et seq., 5240, 8752, 8752.1., and 8758.1.

DOM § 22040.29.

ARTICLE 22 — POLICY AND GENERAL INFORMATION*

Revised October 20, 1994

Not Cleared For Statewide Use

46010.1 Policy

The Department recognizes that EDP equipment represents an indispensable tool for the rapid and efficient handling of data records, communications, and transactions. Also, EDP equipment offers an important potential for increasing the productivity, efficiency, and responsiveness of CDC operations. Maximum efficiency in the use of EDP equipment shall be promoted, and the most cost-effective methods shall be utilized for procurement of EDP equipment.

The relative merits of all methods to acquire and maintain EDP equipment shall be evaluated continuously in order to assure maximum economic advantages for the Department. When selecting EDP equipment, CDC shall consider the requirements for interfacing to present systems. Conversion costs shall also be considered, as well as costs associated with the exchange of information among machines or systems. Unless unusual circumstances warrant otherwise, standard, commercially available, general purpose EDP equipment shall be acquired in preference to specially designed or special purpose equipment.

State-owned EDP equipment shall be used when appropriate, but for only as long as the benefits of such equipment use exceeds related costs. Such equipment shall be used to replace rented or short-term leased equipment installed anywhere within CDC

Duplicate or excess EDP equipment shall not be acquired as insurance against machine failure or as standby equipment, except when legally required or for necessary, full-time, or absolute service functions.

The disposition of EDP equipment determined to be excessive relative to the Department's requirements shall be decided in accordance with the most economical and practical, overall outcome for the Department.

46010.2 Purpose

The purpose of this policy is to establish standards for the use and management of EDP equipment which protect CDC's investment in ITS, promote the identification of cost-effective opportunities for using EDP equipment to support the accomplishment of CDC's mission and program objectives, ensures that the integrity and security of automated files, ITS and program operations are not jeopardized, and create a support structure that provides reliable technical assistance to users of EDP equipment.

46010.3 Definitions

EDP Equipment

SAM 4819.2, defines EDP equipment as:

- Central processing units and all related features and peripheral units, including processor storage, console devices, channel devices, etc.
- Minicomputers, microcomputers, personal computers, and all peripheral units associated with such computers.
- Special purpose systems including word processing, magnetic ink character recognition, optical character recognition, photocomposition, typesetting, and electronic bookkeeping.
- Communications devices used for data transmission such as modems, data sets, multiplexors, concentrators, switches, local area networks, private branch exchanges, network control equipment, and microwave or satellite communications systems.
- Input-output (peripheral) units (off-line or on-line) including: terminals, card readers, optical character readers, magnetic tape units, mass storage devices, card punches, printers, computer output to microfilm converters, video display units, data entry devices, FAXs, teleprinters, plotters, or any device used as a terminal to a computer, and control units for such devices.

Component

A component is defined in SAM 5013 as any individually identified piece of hardware, such as the mainframe, tape drive, disk drive, power supply unit, controller, punch, reader, printer, modem, CRT, keyboard, remote device, and the like.

EDP Supplies

SAM 4819.2 defines EDP supplies as all consumable items and necessities (excluding items defined as EDP equipment) to support information technology activities and EDP personnel including:

- Documents such as standards and procedures manuals, vendor-supplied systems documentation, and educational or training manuals.
- Equipment supplies such as printer forms, punched-card stock, disk packs, “floppy” disks, magnetic tape for EDP devices, and printer ribbons or cartridges.
- Furniture such as terminal tables and printer stands.

46010.4 Integrity of EDP Information

In order to maintain the integrity of EDP information and ensure the security of equipment, the following policies shall be adhered to:

- All EDP hardware and software shall be for official use only.
- Reasonable measures shall be taken to locate equipment in a secure area, to provide protection from vandalism or sabotage, and to preclude access by other-than-authorized personnel.
- All microcomputers located in facilities and parole offices shall be equipped with a keylock mechanism that controls the power source to the processor and disk drives. If a keylock mechanism is not included with the microcomputer, then a keyboard or power lock shall be purchased separately and used. When not in use, the key shall be removed from the lock.
- All microcomputers located in facilities and parole offices shall be associated with locking storage cabinets for software, manuals, and small peripheral equipment. Such equipment shall be secured in the cabinet(s) when not in use.
- A complete set of standard documentation shall be maintained by the individual or unit using the EDP equipment, and shall remain in an area immediately adjacent to the EDP equipment. Such documentation shall include:
  - All manuals supplying documentation relating to the installation, maintenance, or care of the equipment.
  - All manuals supplying documentation relating to the installation and use of proprietary software, except that such manuals may be located in a central library, if appropriate.
- There shall be no inmate access to EDP equipment connected in a Local Area Network (LAN) or having any type of direct, outside communication capability, unless approval is obtained from the MIS Committee and CDCInformation Security Officer.

46010.5 EDP Equipment User Responsibilities

All facilities, parole regions, and units within headquarters that access the CLETS, the DDPS, or the OBIS shall assign an Associate Information Systems Analyst (AISA) or designee to act as liaison between the user locations and ISD of the EC&ISD located in headquarters.

It is the responsibility of each user facility to provide the EDP Operations Manager, ISD, with the name(s) and phone number(s) of its AISA and any designee. In addition, facilities with24-hour shifts shall submit the names and phone numbers of alternate (i.e., off-shift) coordinators to the EDP Operations Manager.

All facilities, parole regions, and headquarters' branches using personal computers shall adhere to the Department's Workgroup Computing Policy.

46010.6 Revisions

The Assistant Director, OOC, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

46010.7 References

SAM §§ 4819.2 and 5013.

ARTICLE 23 — EDP EQUIPMENT MAINTENANCE

Revised October 20, 1994

46020.1 Policy

It is the policy of the Department that EDP equipment shall be maintained in accordance with State requirements and in ways that maximize the operating efficiency of the equipment while minimizing equipment failure and down time. Furthermore, EDP equipment maintenance shall be performed by State personnel, or performed by maintenance service organizations in the private sector whose services are acquired through competitive bidding or as a sole source. Specific criteria for EDP maintenance services shall be defined and applied in the development of procurement specifications. EDP equipment maintenance policies

and guidelines shall be applied in determining appropriate maintenance coverage for EDP equipment installed throughout CDC.

46020.2 Purpose

The purpose of this section is to specify that EDP equipment maintenance shall be performed as required by GC 14816 and SAM 5220.

46020.3 Responsibility for Maintenance of EDP Equipment

CLETS

Maintenance coverage for CLETS equipment is the responsibility of the AISA or designee at the user location involved. Funding for maintenance coverage is the responsibility of the division, facility, or parole region procuring the equipment.

DDPS

ISD is responsible for obtaining maintenance coverage for all equipment associated with the DDPS.

OBIS

ISD serves as liaison among the Teale Data Center, headquarters, individual facilities, and parole locations for the provision of maintenance coverage for all equipment associated with the OBIS.

Paroles Automated System

ISD is responsible for obtaining maintenance coverage for all equipment associated with the Paroles Automated System.

Personal Computers

Maintenance coverage for personal computer equipment shall be obtained in accordance with the Department's Workgroup Computing Policy.

46020.4 Acquisition of Maintenance Services for EDP Equipment Within Department

Acquisition of EDP maintenance services is conducted through competitive bidding except when the Director of General Services determines that the conditions for sole source acquisition are met.

The following conditions are considered justification of sole source acquisition of EDP maintenance service:

Leased Equipment

- Equipment leased from a manufacturer who provides CDC no option but to obtain maintenance for the equipment from that manufacturer.

State-owned Equipment

- Maintenance service for all central processing units (CPUs) except for microcomputers.
- Maintenance of peripheral equipment that is interconnected by cables to CPUs. This does not apply to terminals that are connected to CPUs by communication lines.
- When there is only one qualified maintenance service company within a reasonable distance of the installed equipment.
- When the manufacturer is the only entity with a minimum of six months experience servicing the installed equipment because the equipment has not been on the market a sufficient period of time for others to obtain needed experience.
- When the equipment is under a warranty period.
- When justification does not exist to obtain a sole source a maintenance service contract, CDC shall conduct competitive bidding for the maintenance service as required by guidelines set forth in SAM 5220 through 5255.

CLETS

Maintenance coverage for this equipment is obtained by contracts with county agencies, equipment vendors, or service companies. The method of obtaining the maintenance contract varies depending on the type of equipment being used at the particular location, as well as the manner in which the CLETS service is provided. For assistance in determining the proper method for a specific location, contact the EDP Operations Manager, ISD, EC&ISD, at headquarters.

DDPS

DDPS coverage is provided by a statewide, competitively bid, master contract.

OBIS

OBIS coverage is provided by a master service agreement with the Teale Data Center.

Personal Computers

Personal computer maintenance coverage shall be obtained in accordance with the Department's Workgroup Computing Policy.

46020.5 Revisions

The Assistant Director, OOC, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

46020.6 References

GC § 14816.

SAM §§ 5220 - 5255.

ARTICLE 24 — EDP EQUIPMENT INVENTORY

Revised October 20, 1994

46030.1 Policy

The Department shall maintain an accurate inventory of its EDP equipment, peripheral devices, and software. All purchased EDP equipment shall concur with the technical specifications contained in the SAM 5005. All EDP hardware shall be inventoried at the time of installation, identified with a CDC property tag, and if site requirements necessitate, permanently marked by engraving with the CDC property tag number, item serial number, and DGS billing code number.

46030.2 Purpose

The purpose of this policy is to ensure that CDC is in compliance with SAM 5005 and to provide departmental administrators with an accurate listing of their EDP equipment resources. There shall be a biannual reconciliation of the EDP inventory to update for changes in the system.

46030.3 Inventory Responsibility

CLETS

The local AISA or designee shall be responsible for maintaining an accurate CLETS equipment inventory for the corresponding division, facility or parole region. CLETS inventories shall be forwarded no later than April 1 and October 1 of each year to ISD, EDP operations manager, who shall be responsible for the coordination, compilation, and retention of the departmental CLETS inventory and useful life-cycle schedule.

DDPS

The ISD Operations Support Unit is responsible for maintaining an accurate departmental DDPS equipment inventory. The DDPS inventory shall be forwarded no later than April1 and October1of each year to the EDP Operations Manager, who shall be responsible for the coordination, compilation, and retention of the departmental DDPS inventory and useful life-cycle schedule.

OBIS

The ISD Hardware Unit is responsible for maintaining an accurate departmental OBIS equipment inventory. The OBIS inventory shall be forwarded no later than April1 and October 1 of each year to the EDP operations manager, who shall be responsible for the coordination, compilation, and retention of the departmental OBIS inventory and useful life-cycle schedule.

Personal Computers

Maintenance record keeping for personal computer equipment shall be performed in accordance with the Department's personal computer policy.

46030.4 Documentation for Inventory of EDP Equipment

The EDP inventory shall include the following data elements:

- PrimaryLocation:division/branch, facility, or parole region where equipment is located.
- SecondaryLocation:unit or office where equipment is located.
- BrandofEquipment:monitors, keyboards, printers, etc.
- ModelNumber:monitors, keyboards, printers, etc.
- SerialNumber:monitors, keyboards, printers, software, etc.
- Ownership:whether CDC or specified other owns.
- VersionNumber:software.
- DateofAcquisition:date equipment was received.
- DateofInstallation:date equipment/software was installed.
- DateofRelocation:date equipment/software was relocated.
- RelocationLocation:unit or office where equipment has been relocated.
- Signature:signature of local AISA or designee or AISA'ssupervisor.

46030.5 Revisions

The Assistant Director, OOC, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

46030.6 References

SAM § 5005.

ARTICLE 25 — EDP EQUIPMENT MAINTENANCE RECORDS

Revised October 20, 1994

46040.1 Policy

The Department shall establish a uniform method for recording data pertaining to the repair and maintenance of EDP equipment as required by SAM 5010 through 5015 so as to prevent excessive maintenance costs or any degradation in user and vendor support.

46040.2 Purpose

The purpose of this section is to ensure consistency in reporting, in the capture of data at the time of an incident, and in review by appropriate levels of management of reports made. These are all essential to the effective management and control of EDP equipment maintenance.

46040.3 Responsibility for EDP Equipment Maintenance Records

CLETS

Maintenance record keeping for CLETS equipment is the responsibility of the AISA or designee at each user location involved. Maintenance records shall be forwarded no later than April 1 and October 1 of each year to ISD Data Center for review and analysis of information, and shall be retained by the EDP Operations Manager for as long as the component is in service or there is a possibility of any contractual claim.

DDPS

Maintenance record keeping for DDPS equipment is the responsibility of the ISD Operations Support Unit. Maintenance records for DDPS equipment shall be reviewed and analyzed no later than April 1 and October 1 of each year, and shall be retained by the EDP Operations Manager for as long as the component is in service or there is a possibility of any contractual claim.

OBIS

Maintenance record keeping for OBIS equipment is the responsibility of the ISD Hardware Unit. Maintenance records for OBIS equipment shall be reviewed and analyzed no later than by April 1 and October 1 of each year, and shall be retained the EDP Operations Manager as long as the component is in service or there is a possibility of any contractual claim.

Personal Computers

Maintenance record keeping for personal computer equipment shall be done in accordance with the Department's personal computer policy.

46040.4 Documentation of Maintenance for EDP Equipment

The responsible unit/party shall maintain records of EDP equipment which contain essential data pertaining to repair and maintenance. Such essential data that are required to resolve disputes between the vendor and the Department concerning vendor performance include:

- Document control number: composed of a two-digit year and a two-digit month, followed by a sequence number starting with "one" at the beginning of each month.
- Name of originating facility.
- Name, unit, and phone number of the on-site contact person responsible for taking action to correct a deficiency.
- Date and time the need for maintenance was first noticed.
- Name and phone number of vendor that was notified.
- Dateandtime vendor was notified of problem.
- Dateandtime vendor personnel arrived to repair malfunction.
- Dateandtime component and system were returned to service.
- Identification of affected component/system by manufacturer identification or serial number, and by CDC property tag number.
- Type of service: regularly scheduled preventative maintenance or unscheduled maintenance required to remedy malfunctions or incidents.
- Justification for any delays in the completion of maintenance.
- Description of malfunction or incident.
- Signatures of vendor personnel and a departmental representative.

A maintenance form is to be initiated whenever a system or any component of a system is inoperative because of the need for equipment repair or maintenance, and is to remain open until the problem has been corrected and the component has been returned to service.

46040.5 Revisions

The Assistant Director, OOC, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

46040.6 References

SAM §§ 5010 - 5015.

ARTICLE 26 — DISPOSAL OF EDP EQUIPMENT

Revised October 20, 1994

46050.1 Policy

DGS has approval responsibility for the disposal of all surplus, State-owned and leased EDP equipment including obsolete or inoperable EDP equipment. The Department shall competitively dispose of surplus departmental EDP equipment.

46050.2 Purpose

The purpose of this policy is to ensure that CDC is in compliance with SAM 5951, 8633, and 8640 through 8642 and to ensure that the salvage value of State-owned EDP equipment and purchase option credits for leased EDP equipment are received when doing so is in the best interests of the Department.

46050.3 Responsibility for Disposal of EDP Equipment

CLETS

It is the responsibility of the local AISA or designee to inform ISD, EDP Operations Manager, of any CLETS equipment that requires disposal.

The local AISA or designee shall include the following information in recommendations for disposal of CLETS equipment at the respective facility:

- Manufacturer, type, and model number.
- Model features such as part numbers and descriptions.
- Serial number.
- Present physical condition.
- Present location of equipment.
- Dates of installation and purchase, and funding program.
- Copies of maintenance contracts and relevant maintenance history, such as special maintenance problems or maintenance performance - percentage up-time.

DDPS

It is the responsibility of the local AISA or designee to inform the EDP Operations Manager, ISD, of any DDPS equipment deemed to need disposal.

The local AISA or designee shall include the following information in any recommendation for disposal of DDPS equipment at the respective facility:

- Manufacturer/type/model number.
- Model features, such as part numbers and descriptions.
- Serial number.
- Present physical condition.
- Present location of equipment.

OBIS

It is the responsibility of the local AISA or designee to inform the EDP Operations Manager, ISD, of any OBIS equipment deemed to need disposal.

The local AISA or designee shall include the following information in any recommendation for disposal of OBIS equipment at the respective facility:

- Manufacturer/type/model number.
- Model features, such as part numbers and descriptions.
- Serial number.
- Present physical condition.
- Present location of equipment.

Personal Computers

It is the responsibility of the local AISA or designee to adhere to the Department's personal computer policy.

46050.4 Process and Documentation for Disposal of EDP Equipment

Depending on the applicable EDP equipment, the EDP Operations Manager shall submit at least 30 days prior to the scheduled release date a completed STD Form 152, Property Survey Report, to DGS, Property Reutilization Unit, with an informational copy of the report submitted to the DOF, Office of Information Technology (OIT).

CDC shall, in memorandum form and at least 30 days prior to the scheduled release date, submit an EDP equipment disposal request to the DGS Property Reutilization Unit. The EDP equipment disposal request shall include the following items:

Item Description

- Description of the item to include:
  - Manufacturer, type, and model number.
  - Model features, such as part numbers and descriptions.
  - Serial number.
  - Weight, to nearest pound.
  - Present physical condition.
  - Item location address on the scheduled release date.

Item Historical Information

- Historical Information of item to include:

State-owned EDP Items

- Date of installation.
- Date of purchase.
- Owned by which budget fund.
- Scheduled release date.
- Monthly maintenance costs.
- Type of maintenance contract (attach copy of subject contract Rider B).
- Relevant maintenance history, such as special maintenance problems or maintenance performance -percentage up-time.

Leased/Rented EDP Items

- Date of installation.
- Scheduled release date.
- Current monthly lease price.
- Current list price (supplier current new purchase price).
- Accrued purchase option credits (in dollars) as of the scheduled release date. Separately list any other State financial equity in the item or item features. These credits shall be requested from the supplier and calculated independently by CDC.
- Any financial liability incurred if the equipment is returned to vendor.
- Relevant maintenance history such as special maintenance problems or maintenance performance -percentage up-time.
- How item was procured (e.g., Master Rental Agreement [MRA]). If not MRA-procured, indicate the type of maintenance contract and attach a copy of subject contract Rider B.

CDC Facilitator Identification

- CDC Facilitator identification to include:
  - Facilitator's name.
  - Facilitator's title.
  - Facilitator's unit.
  - Facilitator's telephone number.
  - If equipment is located at a different site, name and telephone number of the on-site contact person.

DGS Disposal

- Proposed DGS Disposition Recommended to include:

If EDP Equipment is State-Owned:

- Transfer or sell to another (named) public agency.
- Scrap for parts for use within (named) State agency.
- Attempt to sell at minimum bid price of (named)dollars.
- Discard the equipment as worthless.
- Justification for no proposed recommendation.
- A completed STD Form 152.

If EDP Equipment is Leased/Rented:

- Transfer equipment to another (named) public agency.
- Release equipment back to the supplier.
- Justification for no proposed recommendation.
- If the EDP equipment was purchased under an MRA, a completed DGS Office of Procurement, GSOP Form 191 and GSOP Form 191A.

Upon approval and instructions from DGS, CDC shall:

If EDP Equipment is State-Owned:

- Transfer or sell State-owned EDP equipment to anotherstate or public agency.
- Follow the determination for disposal of the EDP equipment (signed STD 152). DGS will indicate whether CDC or DGS shall arrange for disposal of the property.

If EDP Equipment is Leased/Rented:

- If MRA-procured, follow the determination for disposalof equipment (signed GSOP Form 191 and GSOP Form 191A).
- If not MRA-procured, take action as indicated by DGS for effecting equipment disposal.

46050.5 Revisions

The Assistant Director, OOC, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

46050.6 References

SAM §§ 5951, 8633, and 8640 - 8642.

ARTICLE 27 — DISPOSAL OF EDP SUPPLIES

Revised October 20, 1994

46060.1 Policy

The Department is committed to ensuring that compliance is maintained with the procedures set forth in the SAM 5951, 8633, and 8640 through 8642 and the GC 14673 through 14675 regarding the disposal of EDP supplies. CDC shall also act in accord with the DGS in its oversight responsibilities for the disposal of all State-owned EDP supplies.

46060.2 Purpose

The purpose of this policy is to effect the efficient and economical disposal of surplus EDP consumable supplies, and to ensure realization by CDC of the maximum salvage value of such supplies to the extent that doing so is in the best interests of the Department.

46060.3 Responsibility for Disposal of EDP Supplies

It is the responsibility of the local AISA or designee to inform the EDP Operations Manager, ISD, of any surplus EDP supplies that the respective facility has deemed to be in need of exchange, transfer, sale, or disposal.

It is the responsibility of the Chief, BSS at headquarters, to act as liaison with DGS for the elimination of CDC's surplus EDP supplies.

46060.4 Procedures and Documentation for Disposal of EDP Supplies

Authorization for the disposal of property shall be received from the DGS Property Reutilization Unit before CDC shall dispose, sell, transfer, or exchange surplus EDP supplies.

DGS administers the statewide master contract for the disposal of wastepaper goods. Use of this contract is obligatory by the Department and is administered by the BSS. Service can also be obtained for the witnessed destruction of confidential records. It is the basic responsibility of CDC to determine that its obsolete records are destroyed in accordance with the requirements of SAM 5951, 8633, and 8640 through 8642. The handling of supplies containing confidential information shall be conducted in accordance with EDP policies regarding confidentiality and security.

CDC shall prepare an STD Form 152, Property Survey Report, when disposing of surplus EDP supplies. The original form shall be marked "Expendable Property" and shall be retained in the CDC Accounting Unit files in order to substantiate the transaction. A copy of the completed STD Form 152 form shall be sent to, and approval shall be received from, the DGS Property Reutilization Unit.

A diligent effort shall be made to secure at least three competitive bids before completion of a sale. In all cases, a list of firms or individuals solicited shall be prepared and attached to, and filed with, the Property Survey Report form. The amount received from the sale shall be accounted as revenue to the fund from which the majority of CDC's support is appropriated.

Surplus magnetic media should: (1) if usable, be transferred to a State agency data processing installation which has a requirement for such media; or (2) be sold by bid if installation personnel are unable or not required to use the media. A list of sources potentially interested in the purchase of used magnetic tape is maintained by the DOF, State Data Processing Management Office. If a sale is not possible, the magnetic media may be disposed of through any dealer or volunteer organization if done without charge to the State.

Prior to disposal or transfer, all magnetic media containing confidential or proprietary data shall be completely magnetically erased; alternately, CDC may overwrite such information with non-confidential, non-proprietary information.

Computer printer ribbons shall be disposed of only when they cannot be reconditioned. Use of a reconditioning or re-inking service for computer printer ribbons is encouraged generally. CDC may contact the providers of such services to discard ribbons with holes or other defects that could produce poor quality or unreadable printout, or may result in subsequent breakage or other unacceptable defect.

When exchanging or transferring EDP supplies free of charge with another State department, CDC shall prepare an STD Form 158, Transfer of Location of Equipment, and shall receive approval from the DGS Property Reutilization Unit before surplus EDP supplies are exchanged or transferred. CDC shall record supplies received free of charge using the same cost basis as that recorded on the books of the transferring department.

46060.5 Procedures for Lost, Stolen, or Destroyed EDP Supplies

Whenever supplies are lost, stolen, or destroyed, CDC shall prepare an STD Form 152 and shall transmit one copy to the DGS Property Reutilization Unit. CDC shall adjust its property accounting records accordingly, and retain the original Property Survey Report form as documentation. This report shall contain:

- A description of the events.
- Precautions to be taken to prevent repeated situations.
- A statement that the CHP or a local law enforcement agency has been notified in accordance with SAM 2625.

Losses of CDC property due to fraud or embezzlement shall be reported to the DOF, Financial and Performance Accountability office, in addition to the law enforcement notification required by SAM 2625. Employees shall be charged with any loss or damage to CDC property due to their negligence or unauthorized use.

46060.6 Revisions

The Assistant Director, OOC, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

46060.7 References

GC §§ 14673-14675.

SAM §§ 2625, 5951, 8633, and 8640-8642.

ARTICLE 28 — OFFENDER BASED INFORMATION SYSTEM

Effective November 25, 1992

47010.1 Policy

The Department shall maintain complete and accurate case records on all prisoners in the custody of the Department as required by PC 2081.5. Case records include all information received by the Department from courts, probation departments, sheriff and police departments, DA offices, the State DOJ, the FBI, and other pertinent agencies and persons.

OBIS was created to provide for automated tracking of all inmates assigned to the Department's jurisdiction from the time of admission through discharge from prison or parole.

47010.2 Purpose

The purpose of this policy is to ensure that complete and accurate records are maintained on all prisoners under the jurisdiction of the Department, and to establish and fix responsibility and accountability for the management of OBIS.

47010.3 Responsibilities

Overall responsibility (e.g., security, data integrity, QA, QC) for OBIS resides with the Director and Chief Deputy Director. Delegated responsibility resides with OISB of the ASD, and with management, supervisory, and end-user personnel involved with OBIS use. OISB is responsible for training data input staff and providing QC oversight to ensure data integrity in OBIS.

As primary users of this system, the case records offices in facilities, parole regions, and headquarters, as well as OISB, input and update offender information in OBIS.

As the custodian of this system, the ISD is responsible for application, hardware, and software support, and maintenance of OBIS.

Parole Violator Work Credit Subsystem

The Parole Violator Work Credit Subsystem records parolee-at-large, parole revocation, and revocation extension information, and applies work credit earned/lost from the inmate work incentive subsystem to calculate violator revocation release dates.

47010.4 Overview of OBIS

Revised July 15, 1993

OBIS is a centralized, on-line, mainframe system that links all facilities, parole regions, selected parole field units, and headquarters to the Teale Data Center. OBIS is the only database which tracks an inmate from initial admission in a state prison through discharge from prison or parole.

Composition Of OBIS

OBIS is comprised of the following subsystems: movement, commitment, descriptive, inmate work incentive; and holds, wants, and detainers.

Movement Subsystem

The movement subsystem records each movement and status change of an inmate from the date of reception from the committing court to discharge from CDC jurisdiction.

Commitment Subsystem

The commitment subsystem records the legal commitment received from the California Superior Court that sentenced the offender to the jurisdiction of the Department.

Descriptive Subsystem

The descriptive subsystem records detailed information regarding each offender's height, weight, hair color, ethnicity, social security number, CII number, FBI number, and date and place of birth.

Inmate Work Incentive Subsystem

The inmate work incentive subsystem is a collection of an offender's applied credits (including vested credits, administrative time, work and vocational assignments, work credit losses and restorations) that affect the release date of the offender.

Inmate Time Collection System

The Inmate Time Collection System (ITCS) is used to track the hours of inmates participating in the IW/TIP. Inmates who participate in the IW/TIP shall earn work time credit toward the reduction of their sentence.

The ITCS introduces a scanning process to the existing time collection system. The scanning system is designed to provide the following:

- Key data entry workload relief for the facility.
- A more expedient method of updating OBIS.

The ITCS scanning process uses revisions of the CDC Form 191, Inmate Timecard, the CDC Form 1697, Work Supervisor Log, and a Sentry 4000 scanner. The work supervisor tracks the inmate work time for a 31 day period, using the CDC Form 1697. Information from the CDC Form 1697 is transferred on to the CDC Form 191. The CDC Form 191 is sent to the case records office for scanning and timecard retention. Scanned information is used to update the OBIS database, and generate error and statistical reports.

Holds, Wants and Detainer Subsystem

The Holds/Wants/Detainer subsystem records holds, wants (warrants), and detainers (HWD) on a particular offender. HWDs are entered on-line immediately after receipt from another agency (e.g., federal, other states) which may have a legal right to hold the offender.

Requests for offender information residing on the OBIS database shall be addressed to the Information System Support and Specialized Reporting Unit, located in OISB.

47010.5 Revisions

Revised April 16, 1993

The Assistant Director, OOC, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

47010.6 References

PC § 2081.5.

ARTICLE 29 — SCO SYSTEMS

Effective November 25, 1992

47020.1 Policy

The Department's Personnel Office shall prepare and release all personnel- and payroll-related data utilizing the SCO Personnel Information Management System (PIMS).

Authorization and guidelines established under the uniform state payroll system are controlled and defined by the Personnel Payroll Service Division within SCO.

47020.2 Purpose

The purpose of PIMS is to ensure that all employee personnel information is considered sensitive and confidential, and that all such data be provided under a strictly controlled environment accessed only as follows:

- The following may be updated, edited, or inquired through the PIMS system: various current and historical information concerning employee status, payment history, or miscellaneous, fixed and voluntary payroll deductions.
- The Personnel Action Request (PAR) is used to access an employee's name, position number, effective date of appointment, salary, range, bargaining unit, and probation status.
- Employee Action Requests (EARS) are used to access an employee's State and federal withholding tax information and home address.

47020.3 Responsibilities

The delegated responsibility for the security, maintenance, monitoring and integrity of the SCO/PIMS system resides with the Personnel Officer at each facility and at headquarters. Major users of the system are Payroll Service Assistants, who audit, provide references, and instruct in preparing PARS and EARS, and Personnel Assistants, who access the system to update all personnel and payroll history. Other users of the system include Personnel Operation Analysts and Personnel Examination Analysts, on an inquiry basis only.

47020.4 Personal Information Management System Equipment Security

Refer to DOM 48010.8 regarding procedures for equipment security.

47020.5 Management Information Retrieval (MIRS) System

CDC uses the Management Information Retrieval System (MIRS) to extract personnel and payroll information from the SCO and to generate supplemental reports for management.

47020.6 MIRS-Reports

Revised April 16, 1993

MIRS supports management decisions by providing the following:

- Payment reports for budgetary analysis.
- Ethnic and gender reports for affirmative action projects.
- Reports to assist with contract negotiations.
- Departmental growth and turnover statistics.
- Current and historical employee data.
- Various employee payment and deduction information.

47020.7 MIRS-Responsibilities

Revised April 16, 1993

The Personnel Automation Unit has delegated responsibility for reviewing personnel report requests. Users refer to the Personnel Action Manual, Payroll Procedure Manual, California State Civil Service Pay Scales for Clarification of Personnel and Payroll Procedures, and the Focus Manual for MIRS programming guidelines. Users log all requests, completion dates, and time spent creating and processing the report.

47020.8 MIRS- Equipment Security

Revised April 16, 1993

Refer to DOM 48010.8 regarding procedures for equipment security.

47020.9 Revisions

The Deputy Director, ASD, and the Assistant Director, OOC, or their designees shall be responsible for ensuring that the contents of this section are kept current and accurate.

47020.10 References

Revised April 16, 1993

SCO: MIRS Manual.

GC §§ 12470, 16390, and 16391 - 16395.

SAM §§ 652 - 660, 4841.5, and 4842.

State of California Personnel Action Manual.

DOM § 48010.8.

ARTICLE 30 — C.L.E.T.S.

Effective November 25, 1992

47030.1 Policy

As a part of its continuing support for all California law enforcement agencies, the Department participates in the statewide telecommunications system developed for use by law enforcement agencies. GC 15150 through 15167 require that State DOJ maintain such a telecommunication system and provide services to California law enforcement agencies when, at their own expense, they require authorized connection to the system.

47030.2 Purpose

The purpose of this section is to describe the relationship between CDC and the CLETS and specify the Department's participation in this system.

CLETS accommodates all public law enforcement user agencies with the capability of providing and receiving fast and efficient point-to-point delivery of messages and information contained in federal and State computerized files. Local information reported to DOJ may also be accessed.

CLETS is a cooperative system whereby the State provides central switching equipment, personnel to staff the switching center, and sufficient circuitry from the switching center to county locations as authorized by law for handling law enforcement message traffic. Department use of the circuitry and terminal equipment extending beyond the CLETS county termination point is provided by CDC.

47030.3 Responsibility

Operational responsibility, system supervision, monitoring of traffic for conformity to rules and regulations, and recommendations for corrective actions are under the direction of DOJ. System rules are designed to provide the most efficient operating system. Adherence to the rules shall provide the Department the maximum effectiveness of CLETS. Violations of these rules shall result in investigative and appropriate disciplinary action. Departmental CLETS coordinators shall direct requests for information concerning the general administration of CLETS to the CLETS Executive Secretary, Department of Justice, P.O. Box 903417, Sacramento, California 94203-4170.

ISD is responsible for coordinating with DOJ the acquisition, relocation and use of the local CLETS. Departmental CLETS coordinators shall direct requests for information concerning changes or additions to CDC's use of CLETS to the EDP Operations Manager, Information Systems Division, P.O. Box 942883, Sacramento, California 94283-0001.

Local facilities are responsible for the funding and maintenance of their CLETS equipment.

47030.4 CLETS- Acquisition Process

Revised April 16, 1993

The acquisition processing time for CLETS varies depending upon the location of the requesting facility: Up to six months should be allowed from the date the request is received for processing at ISD.

It is the local CLETS coordinator's responsibility to:

- Initiate an appropriate request for additions or changes (other than relocation) to CLETS services at an existing location. The request shall include a cover memo to the EDP Operations Manager, ISD, indicating justification for a CLETS addition or change and a completed CDC Form 954, Intraoffice Requisition and Procurement Worksheet.
- Upon receipt of the approved requisition, order equipment and acquire maintenance with facility funding.
- Initiate an authorized request for the relocation of CLETSequipment. The request shall consist of a memorandum with appropriate approval signatures to the EDP Operations Manager, ISD, justifying the relocation.

It is the responsibility of the EDP Operations Manager, ISD, to:

- Review the request, obtain certification approval, and return the completed package to the local facility for their equipment purchase.
- Procure approval from DOJ and appropriate county sheriff's offices for CLETS usage.
- Coordinate CLETS installation with DOJ, county sheriff's offices, and the local facility.
- Notify local CLETS coordinators of approved mnemonic (i.e., "NME") and originating agency (i.e., "ORI") numbers.
- Maintain inventory for departmental CLETS circuitry.
- Review requests for, and coordinate the relocation of CLETSequipment.

Terminals connected directly to CLETS shall be approved by DOJ. A hard copy printer shall be included with each terminal authorized to receive unsolicited or point-to-point, non-data-base traffic.

47030.5 Integrity of CLETS Information

In order to maintain the integrity of CLETS and ensure the security of information received and transmitted by use of the system, the following policies shall be adhered to:

- Reasonable measures shall be taken to protect equipment from vandalism or sabotage and preclude access by other than authorized personnel by locating equipment in a secure area.
- Mobile digital terminals shall not be allowed to access DOJ'scriminal history system.
- Personnel authorized to access CLETS are either sworn law enforcement personnel or nonsworn law enforcement personnel that have been subject to a character or security clearance. The clearance shall include the following:
  - DMV: drivers license check.
  - DOJ: fingerprint check.
  - CDC: background investigation. An agency head's authorization for the employee to operate CLETS equipment shall be placed in the employee's personnel file.
  - In all matters pertaining to personnel security, the agency head shall be responsible for making the final determination of the individual's suitability for the job.

All CLETS messages are confidential and for official use only. Examples of acceptable messages are:

- Requests for record validation.
- Requests for prisoner pickup and transportation.
- Requests for mail-back information from data bases.
- Information regarding the circumstances surrounding the death of an officer killed in the line of duty.
- Listings of stolen property when identifiable by serial numbers or unique markings.
- All subpoenas transmitted by CLETS shall be processed in accordance with PC 1328(b) and 1328(c). A subpoena relative to civil proceedings or any subpoenas which could be delivered in a timely manner by other means are not acceptable for transmission.

DOJ publishes manuals for CLETS operators containing information for proper system utilization. These manuals shall be obtained and maintained for CLETS operators.

47030.6 CLETS-Training/Coordinators

Revised April 16, 1993

Each facility, parole region, and headquarters' division shall provide the EDP Operations Manager, ISD, with the names and phone numbers of their CLETS coordinator. In addition, facilities with 24-hour shifts shall submit the names and phone numbers of alternate (off-shift) CLETS coordinators.

It is the equipment vendor's responsibility to provide training on the operation of their terminals when initially procured/installed.

It is the responsibility of State DOJ field service/training office to provide training for information access in the:

- Criminal justice information system data bases.
- National crime information center.
- National law enforcement telecommunications system.
- DMV.
- Oregon law enforcement data system.

Local CLETS coordinators should call the specified telephone number for the name and telephone number of their DOJ field service/training representative.

47030.7 Revisions

Revised April 16, 1993

The Assistant Director, OOC, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

47030.8 References

GC §§ 15150 - 15167.

PC §§ 1328(b) and 1328(c).

ARTICLE 31 — PERSONAL COMPUTER SYSTEMS

Effective November 25, 1992

47040.1 Policy

It is the policy of the Department to provide, where appropriate, personal computer personal computer applications as an alternative to other types of information technology or manual systems. Ease of maintenance, cost effectiveness, and efficiency are major considerations in determining the use of personal computers. Security is the primary policy consideration in initiating and maintaining all personal computer systems with sensitive information.

47040.2 Purpose

The purpose for utilization of personal computer systems is to meet departmental needs that are not addressed effectively or efficiently by other means. Systems geared basically to intrafacility needs, and not for the purpose of sharing application and data files or databases, frequently lend themselves to low cost, effective, personal computer systems.

47040.3 Responsibility

It is essential that confidential data bases are not broached by unauthorized personnel. It is the responsibility of Wardens and Regional Administrators and their designees to maintain surveillance in order to assure this does not occur and that requirements for security in this area are met.

Additionally, there is a responsibility by all persons supervising the system or with access to it to maintain an acceptable standard of QA and QC. This may be accomplished by user groups, departmental audits, supervisory vigilance, and other specified methods appropriate to the system.

Descriptions of the personal computer systems currently maintained in the facilities are provided in this section. These systems are the responsibility of the persons designated in the DOM 47040.3, as well those specifically named in each system described below.

The programs are designed for personal computers on a statewide basis. Responsibility for maintaining these systems is the responsibility of ISD.

47040.4 State Logistics and Material Management

Policy

CDC policy requires accountability in the expenditure of funds. This includes the accumulation of supplies and equipment, and inventory related to expenditures.

Purpose

The purpose of the State Logistics and Material Management System (SLAMM) is to provide a system of accountability for, and current information in, the tracking of inventory in the facilities.

Systems Description

SLAMM is an inventory control system. It was designed to provide facilities with accurate and up-to-date data on their inventories. It has been implemented statewide.

SLAMM can produce various reports on all items entered and maintained in the system. Information may be viewed or updated on-line. The program helps the facilities maintain inventory information and better manage resources.

SLAMM information is retained on both a master file and a transaction file. The master file is automatically updated as transactions are entered. The transaction file is maintained on a current fiscal year basis only.

Responsibility

All facilities are required to maintain their warehouse inventories on this system. The program is the shared responsibility of ISD and the Department's materials manager. Security and data integrity for SLAMM information is the responsibility of the warehouse manager.

47040.5 FLSA Program

Policy

This program was designed to meet the requirements of the FLSA with regard to overtime payment. It is the policy of CDC to comply in an efficient and accurate manner with federal requirements for FLSA.

Purpose

The FLSA program is a statewide program designed to do the precise and complex calculations required by the FLSA with regard to the payment of overtime.

System Description

Appropriate formulas relating to overtime and shift time are included in this computer program to arrive at an accurate and rapid calculation of overtime pay.

Responsibility

Each facility shall use this program in the computation of overtime pay. The facility's personnel officer is responsible for data integrity and overseeing that

security is strictly maintained in regard to all confidential information contained in this application.

47040.6 Inmate Appeals Tracking System

Policy/Purpose

The Inmate Appeals Tracking System (IATS) is a statewide system that was designed to allow up-to-date, comprehensive information with immediate access to appeal coordinators on all activity pertaining to appeals cases.

System Description

IATS generates lists of log entries by various parameters. In addition to printing "lost notices" for inmates, IATS prints route slips and overdue notices for reviewers and inmates. IATS also provides a method for accurate tracking of due process times.

Other features of IATS include monthly statistical reports for in-house use and quarterly reports for submittal to CDC headquarters.

This system has been implemented on a statewide basis. Strict security maintenance is required for IATS and is the responsibility of the facility's Inmate Appeals coordinator. Inmates are not permitted access to the IATS system in any of its aspects.

Responsibility

Headquarters' responsibility resides with the Chief, ISD, and the Inmate Appeals Branch. Facility responsibility rests with the appeals coordinator.

47040.7 IST Program

Policy

The IST Program maintains records on training courses being offered and attended in the facilities. It is the policy of CDC to provide facility management and staff with accurate data on available training.

Purpose

The purpose of this application is to increase accuracy in reporting and to follow-up on employees taking IST courses.

System Description

The IST program is a statewide program that provides information sorted by staff member, instructor, and class title on courses being attended in the facility. It also tracks requirements for range qualifications, and sorts courses by instructor. In addition to the data collected on individuals, it provides some summary information.

Responsibility

Responsibility for security and for accuracy in reporting for this program rests with the IST coordinator in the field. Headquarters' responsibility resides with the Chief, ISD.

47040.8 Personnel Post Assignment System

Policy

It is the policy of CDC to adopt the Personnel Post Assignment System (PPAS) to standardize the operations within the personnel, personnel assignments, timekeeping, and accounting units.

Purpose

The purpose of PPAS is to:

- Provide a flexible authorized post assignment schedule.
- Track daily employee attendance.
- Provide immediate access to employee job histories.
- Provide monthly billing reports for the accounting unit.
- Provide automatic placement of employees into job assignments.
- Track day-by-day work history with complete recall and review.
- Provide accurate timekeeping data to release payrolls.

Responsibility

The Personnel Automation Unit has the delegated responsibility for installing, implementing, and providing user support. Primary users of PPAS are personnel assistants who enter all employees' hire dates, seniority dates, job classifications, and salary. Personnel assignment staff enter all information for each custody position created at the facility, including work hours, watch, regular days off, lunch, daily assignments, sign-in area, master roster location, supervisors post number, and division number. Custody timekeepers are responsible for the recording and tracking of each employee's daily attendance records and overtime. The accounting unit shall utilize the overtime breakdown to estimate and calculate data for the CALSTARS billing report.

Equipment Security

To ensure the security of PPAS equipment and information, employees shall adhere to the following equipment security guidelines:

- Equipment shall be located in restricted areas that are monitored during working hours and locked during any unattended periods.
- Only authorized employees shall have access to terminals, printers, control units, and modems.
- System access shall be completely signed off when not in use.
- Terminals shall be locked, keys removed, and screen intensity turned completely down when the terminals are unattended.

The following shall be stored in a vault or locked cabinet when not in use:

- Keys to terminals.
- Manuals on the system software and hardware.
- Other instructional and operational manuals.

47040.9 Revisions

Revised April 16, 1993

The Deputy Director, ASD, and the Assistant Director, OOC, or their designees shall be responsible for ensuring that the contents of this section are kept current and accurate.

47040.10 References

Revised April 16, 1993

FLSA

Senate Bill 16, Stats. 1987, ch. 1435.

DOM §§ 47040.3 and 55070.4.

Personnel Post Assignment User's Manual.

ARTICLE 32 — SELECTION AND STANDARDS TRACKING SYSTEM

Revised April 16, 1993

47050.1 Policy

The Selection and Standards Branch (SSB) has the delegated authority from the SPB to test certain classifications used primarily by the Department. The SSB, through an on-line database at the Teale Data Center, shall monitor the application, acceptance/review, written/oral testing, medical testing, and background investigation for the Officer, CC-I, MTA, PA-I, and other peace officer reinstatement classifications.

47050.2 Purpose

The main purpose of this system is to track the applicants through the various phases of the testing process and to provide written statistics and status reports to management.

47050.3 Responsibility

The Department's ISD has the delegated responsibility for implementing, installing, and providing user support.

The data entry and training responsibility for the system are managed by SSD. The system is designed to track the applicants through the full testing processes. As each applicant passes the written and oral examination(s), data and results are recorded and the applicant proceeds to the preliminary physical testing. As the various testing results are defined, the data are recorded to monitor and provide management with workload data. When necessary, system updates and management reports are created weekly, daily, monthly, and annually.

Enhancements to the system are submitted to ISD on an ongoing basis. Data processing applications and future needs are discussed and prioritized by ISD and SSB on a workload basis and as resources are made available.

47050.4 Revisions

The Deputy Director, ASD, and the Chief, ISD, or their designees shall be responsible for ensuring that the contents of this section are kept current and accurate.

47050.5 References

None.

ARTICLE 33 — INCIDENT REPORTS DATABASE

Revised April 16, 1993

47060.1 Policy

It is the policy of the Department to provide statistical information on all reportable incidents within California's correctional facilities that involve felons or

civil addicts. DOM 51030 defines incidents required to be reported to The Director.

47060.2 Purpose

The purpose of this policy is to establish and fix responsibility and accountability for the management of this system.

47060.3 Responsibility

Overall responsibility for the incident reports database (e.g., security, data integrity, QA, QC) lies with The Director and Chief Deputy Directors. Delegated responsibility resides with OISB. TSS within OISB is responsible for receiving, analyzing, and coding all reportable incidents; entering the incidents into the database; maintaining incident reports; and ensuring incident reports data base QC.

The Estimates and Statistical Analysis Section of OISB is responsible for the creation of statistical summary reports, annual and quarterly publications, and ad hoc requests.

47060.4 Incident Reports Database-Overview

The incident reports data base is a mainframe system which utilizes personal computers for initial data entry and ultimately uploads the data to a mainframe computer at the Teale Data Center for batch processing. The data are then manipulated and processed for various statistical and informational purposes.

Incident reports are submitted to the Institutions Division in headquarters and OISB staff within 72 hours of the occurrence of the incident. Upon receipt, OISB staff date stamp and manually log the incident report into the incident log book. Data are then extracted from the incident report and a coding sheet is completed. The information from the coding sheet is then entered into the personal computer-based incident reports data base and uploaded to the mainframe system.

47060.5 Revisions

The Assistant Director, OOC, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

47060.6 References

DOM § 51030.

ARTICLE 34 — REVOCATION TRACKING SYSTEM

Revised April 16, 1993

47070.1 Policy

CCR (15) (2) BPT Rules, states that parolees shall be afforded timely completion of the revocation process within a 45-day time frame.

The BPT and the Department designed the Revocation Tracking System (RTS) to meet these crucial time requirements. RTS contains detailed information on all parolees who are under CDC hold (or a discovery action if allowed to remain in the community) and who are being processed for revocation. The tracking begins at the date of hold (or discovery) and ends with a decision by the BPT.

47070.2 Purpose

The purpose of this policy is to ensure that accurate and timely tracking of parolees, pending revocation of parole, is maintained by CDC in conjunction with the BPT.

47070.3 Responsibility

At the present time, overall responsibility for the RTS resides with the Director and Chief Deputy Directors of CDC, and with the Chairman of the BPT. This responsibility is presently delegated jointly to the CDC Deputy Director, P&CSD, and the Chief of Administrative Services, BPT. These latter individuals have specific responsibilities for QC and QA. Parole regional office staff who input data have primary responsibility for data accuracy, integrity, and system security.

47070.4 Revocation Tracking System Overview

RTS is a centralized, on-line mainframe system which links all facilities, parole regions, and the BPT to the Teale Data Center.

RTS is comprised of descriptive information that identifies the parolee by name, CDC number, and parole unit, as well as by status information relevant to the pending charges such as hold date, current location, and booking number. The system also tracks deadline information such as signature, screening and service dates, and scheduling information regarding where, when, and what happened.

47070.5 Revisions

The Chief, ISD, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

47070.6 References

CCR (15) (2) BPT.

ARTICLE 35 — OFFICE VISION SYSTEM

Revised April 16, 1993

47080.1 Policy

It is the policy of the Department to automate manual information transfer functions whenever and wherever it is cost effective to do so.

47080.2 Purpose

The purpose of this policy is to maximize efficient use of the Department's human resources, when possible, through the use of automated systems. To this end and to help eliminate the inefficient use of time and money involved in non-contact phone calls (especially long distance), electronic mail and document transfer capabilities have been adopted. This data transfer and storage system, known as "Office Vision," is designed to hold and deliver on-request notes, messages, and documents among those authorized to use the system.

47080.3 Responsibility

The CDC Director has overall responsibility for the use and function of the system. Delegated responsibility for use resides with the Deputy Directors of each division and their designated managers. The Chief, ISD, is responsible for the technical and overall management of the system within the Department.

Technical security of this system is centralized at the Teale Data Center (TDC), while the administration of security is accomplished by the ISD security unit. Through subsystem commands, the security unit adds and deletes users as necessary for the efficient administration of the system.

Since this is a free-form text entry system, data integrity and accuracy are provided through the security of log-on identification, integrity of the data storage area, and routine data backups to tape by TDC.

Each major unit using this application shall designate a single contact person who shall provide coordinator and liaison functions between the end user and the OfficeVision administration unit in ISD. User additions, deletions, or changes shall be forwarded to the administration unit by OfficeVision mail, or by memo, before any maintenance to the system may occur.

47080.4 Office Vision- Overview

OfficeVision is used by client departments such as CDC by a wide area network. Each department has the responsibility to administer its own use of this application. The system currently has approximately 23,000users in 20 client agencies, and allows for the electronic sending and receiving of notes, messages, and documents (mail). The system holds and tracks all incoming and outgoing mail for the user's review. Mail may be revised and retransmitted to another person, printed to any printer, or held in an electronic file for indefinite periods of time.

Within the OfficeVision application are menu-driven sub-applications of spreadsheets, status, and personal financial functions. These are available to any authorized user at additional cost to the Department.

47080.5 Revisions

The Chief, ISD or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

47080.6 References

None.

ARTICLE 36 — PIA SYSTEM*

Effective November 30, 1992

Not Cleared For Statewide Use

47090.1 Policy

PIA was created by Senate Bill (SB) 1574, Stats. 1982, ch. 1549. The intent of the Legislature in enacting SB 1574 was made explicit within the language of the bill:

- "The constraints of state government severely impede the ability of the prison industries program to operate on a self-supporting or profit-making basis."
- "A successful prison industries program can best be accomplished by providing the management of the prison industries program with a reasonable degree of autonomy and by establishing a special authority to manage and operate prison industries and the funds associated with such programs."

In December of 1984, PIA asked the Attorney General for a legal opinion relating to the Office of Information Technology (OIT) oversight role and the SAM requirements pertaining to data processing activities within PIA. After a review of

PC 2808(g), the Attorney General found that the responsibilities of OIT would constrain PIA's ability to establish its own procedures for the purchase of data processing goods and services, and rendered the opinion that PIA does not fall under the oversight responsibilities of OIT. Therefore, the provisions of SAM 4800 through 5999 do not apply to the PIA.

47090.2 Purpose

The purpose of this policy is to utilize automation for a variety of PIA business activities to reduce administrative costs and to improve service to it's customers.

47090.3 Responsibility

Revised April 16, 1993

The Director has overall responsibility for all data processing systems within PIA with delegated responsibility given to the PIA General Manager. This latter responsibility is further delegated within PIA depending on the subsystem involved.

Security

Within the facilities, PIA utilizes personal computers for various business activities. Since the Warden has ultimate responsibility for the security of the facility, PIA's lead production managers shall report any security violations involving the use of personal computers by inmates to the Warden, or designee (usually the Associate Information Systems Analyst). In addition, security violations shall be reported to the PIA Information Security Officer in headquarters. Such security violations shall then be reported to the Department's Information Security Officer by PIA's Information Security Officer through the same process used to report security violations within the Department.

In March of 1988, an on-line system was approved for use by PIA to allow inmate access. This system utilizes a central, stand-alone computer in PIA headquarters. "Dumb terminals" (i.e., terminals with no central processing unit) are used to communicate with the PIA computer, located at PIA headquarters, by dedicated phone circuits, controllers, and modems located in the facility. The signals sent through the dedicated phone circuits are encrypted. The controller, modem, and encryption devices located in the facility shall be kept in a locked box in an area out-of-bounds to inmates.

Violations associated with computers in PIA headquarters shall be reported to the PIA Information Security Officer. If these security violations involve an inmate employed by PIA headquarters, they shall be reported to the Department's Information Security Officer.

PIA's Lead Production Manager shall advise the Warden or designee prior to installation of any EDP-related equipment. Personal computer purchases shall require approval by the Warden as indicated on the PIA personal computer request form. For other equipment, the Production Manager shall notify the Warden or designee as soon as the Production Manager is aware of the planned installation date.

Data Integrity

(Reserved).

QA/QC

(Reserved).

47090.4 Reserved

Revised April 16, 1993

(Reserved).

47090.5 Revisions

Revised April 16, 1993

The Chief, ISD, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

47090.6 References

Revised April 16, 1993

SB 1574, Stats, 1982, ch. 1549.

PC § 2808(g).

SAM §§ 4800 - 5999.

ARTICLE 37 — CLASSIFICATION TRACKING SYSTEM

Revised April 16, 1993

47100.1 Policy

It is the policy of the Department to adhere to the provisions of PC 2081.5 which require that the Department maintain complete and accurate case records on all prisoners in its custody. Each case record file shall include all information received by CDC from courts, probation departments, sheriff and police departments, DA offices, the State DOJ, the FBI, and other pertinent agencies and persons.

The Classification Tracking System (CTS) was developed to automate the paper-flow process associated with classifying and maintaining a complete (classification) history of an inmate.

47100.2 Purpose

The purpose of this policy is to establish and fix responsibility and accountability for management of CTS.

47100.3 Responsibility

Overall responsibility (e.g., security, data integrity, QA, QC) for CTS lies with the CDC Director and Chief Deputy Director. Delegated responsibility resides with OISB, and with management, supervisory, and end user personnel for units that utilize the applications residing on CTS.

As custodian of the system, ISD is responsible for application hardware, software support, and maintenance of the system.

47100.4 Classification Tracking System-- Overview

CTS is a batch processed, centralized inmate classification system supported by the Teale Data Center. CTS contains a complete historical record of all classification information for all inmates and parolees under CDC jurisdiction.

Facility staff shall forward a copy of each CDC Form 839, Initial Classification Score Sheet, and CDC Form 840, Reclassification Score Sheet, to OISB for data entry. TSS reviews all classification documents, coordinates data entry with the agency providing the key entry contract service, and acts as liaison with ISD on the weekly update of the system. TSS and facility classification staff conduct regular joint OISB/facility data reviews to maintain the accuracy and integrity of CTS data. In addition, TSS provides CTS QC training, coordinates requests for changes and improvements to the data system, and responds to requests for classification data from facilities, parole regions, headquarters, and outside agencies.

The Estimates and Statistical Analysis Section uses CTS information to generate monthly summary reports and semiannual reports on inmate classification scores, classification levels, and projected bed needs by classification level. Summary information is extracted from CTS for use in planning and decision making in the Department and by control agencies. Projected bed need information is used by the Department for budgeting and planning new prison construction. CTS information is also used to answer requests from Department staff and others on various characteristics of inmates, such as the number of felons with holds, special category needs, or military service.

Requests for specialized reports and other offender information shall be addressed to TSS in OISB.

47100.5 Revisions

The Chief, ISD, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

47100.6 References

PC § 2081.5.

ARTICLE 38 — POSITION AND AUTOMATED LEAVE SYSTEM

Effective November 30, 1992

47110.1 Policy

The Department has adopted an on-line Position and Automated Leave System (PALS) from Teale Data Center for administration and paroles. Expansion to the facilities shall be based on funding available from individual facilities.

47110.2 Purpose

The primary purpose of this system is to alleviate manual attendance keeping, reduce a substantial amount of clerical duties needed to report attendance, and provide accurate records with up-to-date personnel information for management and employees. PALS is designed to aid the personnel office staff in posting, calculating, auditing, and correcting attendance, and tracking position roster maintenance. PALS eliminates the need to maintain and file hard copy records. The system provides flexibility to accommodate bargaining unit contract changes, employee benefits, and legislation. Management may utilize the system to receive position listings by employee name, division, unit or class. Also available are vacancy, blanket, overtime, and various tickler reports.

47110.3 Responsibility Within PALS

The Personnel Automation Unit has the delegated responsibility for implementing and providing user support. Major users of the system are timekeepers who input employee leave data, personnel assistants who input personal employee history (i.e., name, social security number, home address, etc.), and audit and balance

timekeepers, who input and maintain position roster controls. Automation analysts and programmers program and test PALS.

47110.4 Equipment Security for PALS

To ensure security of PALS equipment and information, employees shall adhere to the following equipment security guidelines:

- Equipment shall be located in restricted areas that are monitored during working hours and locked during any unattended periods.
- Only authorized employees shall have access to terminals, printers, control units, and modems.
- System access shall be completely signed off when not in use.
- Terminals shall be locked, keys removed, and screen intensity turned completely down when the terminals are unattended.
- The following shall be stored in a vault or locked cabinet when not in use:
- Keys to terminals.
- Manuals for the system software and hardware.
- Other instructional and operational manuals.

47110.5 Revisions

Revised April 16, 1993

The Deputy Director, ASD, and the Chief, ISD, or their designees shall be responsible for ensuring that the contents of this section are kept current and accurate.

47110.6 References

PALS User's Manual.

ARTICLE 39 — STATEWIDE ACCOUNTING AND REPORTING SYSTEM

Effective November 30, 1992

47120.1 Policy

It is the policy of the Department to use the California Statewide Accounting and Reporting System (CALSTARS) to perform program cost accounting, provide financial information for management, and help standardize the State's accounting process.

47120.2 Purpose

CDC uses CALSTARS in order to:

- Provide timely, accurate, and meaningful financial information.
- Streamline user access to accounting information, and the processing of accounting transactions.
- Provide financial information reports for management purposes.
- Satisfy legal requirements of accounting for the State's resources at the Department and facility level.
- Have the capability to meet the State's reporting requirements.

47120.3 Responsibilities

The DOF has overall responsibility to maintain and enhance the capabilities of the CALSTARS system.

Operational and financial responsibilities for CALSTARS have been delegated to the fiscal officers at CDC facilities. These fiscal officers shall ensure the following:

- Accounting staff understand CALSTARS' accounting process.
- All financial data entered into CALSTARS' system are accurate and entered in a timely manner.
- CALSTARS' reports are reviewed for accuracy.
- Management is provided with accurate financial data.

The Accounting Systems Section is responsible for:

- Assisting, resolving, and making recommendations regarding CALSTARS' system problems.
- Monitoring CALSTARS' operations at each facility's accounting office.
- Installation and implementation of CALSTARS systems for new facilities.
- Providing detailed CALSTARS accounting training.

Security

In order to operate CALSTARS, designated personnel within the Department shall be provided with the ability to access the system through CALSTARS terminals within the Department. Each accounting office shall designate an individual as the security officer. This individual may be the person in charge of accounting, or an individual at a higher level. The security officer is required to:

- Complete CALSTARS Form 95, Security Form, to assign each designated person a user identification name. In the completion of this form, the individuals are assigned access only to those areas that affect their particular job responsibility. This form shall be submitted to the CALSTARS EDP section of DOF in a sealed envelope marked "confidential."
- Complete and submit a CALSTARS Form 98, Signature Sheet, to CALSTARS EDP Section at the DOF.
- Ensure that there is proper separation of duties within the Department, as required by the SAM 8080.1.
- Complete CALSTARS Form 95 to add, change, or delete records in the security file as changes occur.
- Maintain a listing of all departmental personnel assigned to CALSTARS user identification. A listing of CALSTARS' users by the Department is available by special request from the DOF.

47120.4 Overview of California Statewide Accounting and Reporting System

CALSTARS is a comprehensive and flexible system that has been designated to satisfy most of the accounting and reporting requirements of the Department. Listed below are the accounting functions CALSTARS performs.

Appropriation Accounting

Encompasses controlling the financial activity of the Department at the level specified in the budget act and by other pertinent legislation. The primary objective of appropriation accounting is to assist the Department by ensuring that expenditures stay within legal limitations.

Allotment Accounting

Encompasses two functions: first, to prevent expenditures from exceeding certain budget allotments; second, to help monitor internal budgets established to report on Department operations.

Budget Preparation Support

Provides historical data needed for budget preparation.

Encumbrance Accounting

Provides accountability of each encumbrance document, safeguards against the over-expenditure of funds, and tracks the status of each encumbrance document and any related actions against it.

Claim Processing/Disbursements

Provides automated support in the preparation and processing of claim schedules for payment to vendors.

Obligations/Accounts Payable

Facilitates the reporting of obligations incurred. Each obligation can be tracked by document number.

Receipt Accounting

Classifies and records all monies received by the Department.

Accounts Receivable

Maintains information on accounts receivable to assist in tracking amounts due to the Department.

Office Revolving Fund

Provides data to support the revolving fund operation by tracking individual advances, and by providing the ability to account for and report on all of the assets, liabilities, and transactions of the revolving fund.

Federal Grant Accounting

Provides detailed cost accounting for each individual grant.

General Ledger Accounting

Maintains separate general ledger accounts to indicate balances of the various types of assets, liabilities and residual nominal accounts.

Cost Accounting/Cost Allocation

Provides automated assistance in the allocation of indirect costs to programs.

Labor Distribution

Provides personnel costs to programs through the State Controller's payroll interface tape.

Report/Retrieval

Provides standard financial reports and has ad hoc reporting capability.

47120.5 Revisions

Revised April 16, 1993

The Chief, ISD, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

47120.6 References

SAM § 8080.1.

ARTICLE 40 — DISTRIBUTED DATA PROCESSING SYSTEM

Revised April 10, 1993

47130.1 Policy

It is the policy of the Department that the DDPS be used by facilities to efficiently maintain specified inmate information. This on-line, integrated information system has been established at the facilities to allow information sharing among multiple users within each facility.

47130.2 Purpose

The purpose of this policy is to describe DDPS and provide requirements for its use, thereby assisting facility staff to maintain a more efficient and secure environment in facilities.

47130.3 Responsibility Within DDPS

Wardens have direct responsibility for the use of DDPS at facilities, and responsibility is delegated to staff who use DDPS applications. Such responsibility includes ensuring the security of the system, and the integrity and accuracy of its data.

Users input information into the DDPS and, in return, are able to access the pooled information data base of the system. Since multiple users access the data base, there is an increased importance for entered information to be timely and accurate since it is relied upon by users throughout the Department.

The facility AISA is responsible for on-site support of DDPS users. This includes user log-on, security, trouble-shooting, producing ad hoc reports using INFORM, personal computer download activities, and headquarters liaison activities. The AISA provides assistance and training to users of the system. Additional training and assistance may be arranged through ISD.

DDPS issues that cannot be resolved at the facility or through ISD should be directed to the Deputy Director, ID.

QA and QC are ongoing concerns. ISD has established controls to ensure the accuracy of technical aspects of DDPS. Periodic monitoring and audits have been established to ensure that QC requirements are met, and assistance is provided to eliminate deficiencies within specified time frames.

47130.4 System Overview of DDPS

DDPS is a system comprised of one or more minicomputers operating in each facility and connected to minicomputers in headquarters by a wide area communications network. Four major applications reside currently on the DDPS. In addition to the requirements of this section, use of each application shall meet general operating specifications regarding policy, purpose, responsibility, QA, and QC.

The four DDPS applications are:

Inmate Roster System

The Inmate Roster System is the basis for DDPS and is, therefore, critical for the maintenance of all other DDPS applications. The roster is designed for use by control room staff and provides an automated means for tracking inmate location. This application allows any authorized user to request reports or make inquiries regarding any inmate or housing unit in the facility.

Inmate Roster Record

An Inmate Roster Record is created the first time an inmate is admitted. At that time, control room staff enter the inmate's full name, date of birth, ethnicity, arrival date, and location from which the inmate arrived. Once the inmate is admitted, the user must enter only the inmate's CDC number and the first five characters of the last name to enter a movement transaction. Reports on inmate movement may be generated within this application. The Automated Daily Movement Sheet is designed to assist control room staff in their use of the CDC Form 117, Daily Movement Sheet.

In addition to the inmate roster, this application maintains a roster of the housing structure and beds at each facility. Control room staff may use this information to readily identify vacant beds, the identity of the inmate in each bed, and beds that are being held for inmates on temporary leave from the facility (e.g., out to court for the day, in a local hospital). Bed vacancy and empty bed reports may be produced in this application to assist control room staff with the running count process.

Although the inmate roster was designed to serve the needs of control room staff, it has proven to be highly beneficial to other functional areas of the facility. Mailrooms have replaced their card systems with query terminals, and many visitor control areas use either terminals or housing reports to locate inmates within the facility. The inmate assignment office uses the information to make appropriate job assignments. Facility staff can request the preparation of special reports by their AISA using "INFORM" or by ISD using ad hoc reporting capabilities.

Responsibility

The Control Room Sergeant is responsible for data integrity and security of this application.

Time Collection System

The Time Collection System automates the data entry portion of updating the OBIS work time credit database. The CDC Form 191, Inmate Timecard, is scanned using a Sentry 4000 Optical Scanner. The scanned timecard information is sent to a file on the DDPS at each facility; the file is transferred nightly to Teale Data Center; data is validated; and the OBIS database is updated.

Responsibility

The CCRM is responsible for data integrity and security.

Inmate Classification System

The Inmate Classification System tracks the results of inmate classification hearings and contains certain descriptors critical to other functional areas of the facility. The privilege group determines an inmate's eligibility for canteen draw, visiting, and other inmate activities. Additionally, the inmate classification system tracks hearing dates and provides a "tickler" to notify counselors of upcoming hearing responsibilities.

Inmate Classification System information is entered after the initial inmate record is created. It is imperative to enter data during or immediately following hearings so that staff have up-to-the-minute information about a inmate's custody level and classification score, thus assisting subsequent program decisions.

Responsibility

The CC-II/III is responsible for data integrity and security.

Inmate Assignment System

The Inmate Assignment Application tracks inmate job assignments and inmate job waiting lists. It contains descriptive information about each job, including pay grade, dictionary of occupational titles code, Inmate Work Training Incentive Program code, assignment beginning date, job status, work location, site phone number, work schedule including regular days off, the name of the inmate holding the job if assigned, and any restrictions or special job requirements.

When assigning an inmate to a job or a waiting list, this application uses the Inmate Roster Record (including classification information) to draw custody level and suffix, work group, ethnicity, administrative determinants, work qualifiers, and housing data.

Information entered by the assignment lieutenant updates the inmate roster clearance regarding food handling, gate clearance, and other clearances. The Inmate Assignment System maintains a inmate's current work and waiting list status. Job history records provide information (including dates) about all previous jobs held by an inmate in that facility. Location records provide ethnicity counts to assist in maintaining an ethnic balance. Transportation records contain assignment information used for the daily movement sheet.

Responsibility

The Inmate Assignment Lieutenant is responsible for data integrity and security.

Inmate Trust Accounting System

PC 2085 and 5057 require that the Department establish, as necessary, an accounting and auditing system to accurately account for all inmate money and property. The Inmate Trust Accounting System is designed to:

- Replace outdated bookkeeping machines.
- Automate the bookkeeping functions in the facility's trust office.
- Account for all inmate monies held in trust by the Department. Each facility uses the inmate trust account system to perform trust accounting functions.

This application uses information provided by the Inmate Roster System to identify inmates who have just arrived, transferred out, transferred in, or have been paroled or discharged. For each new arrival, the Inmate Trust Accounting System establishes a trust account in which monies shall be held and deposits and withdrawals posted. An inmate's record is updated when the inmate leaves the facility to reflect the new location so that account information and funds can be transferred.

The Inmate Trust Accounting System produces monthly statements of account, a general ledger, accounts payable, accounts receivable, a daily balance sheet, audit reports, and preprinted canteen cards.

Responsibility

The Trust Officer is responsible for data integrity and security.

47130.5 Revisions

The Chief, ISD, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

47130.6 References

PC §§ 2085 and 5057.

ARTICLE 41 — DEPARTMENTAL WORKGROUP COMPUTING POLICY

Revised March 21, 1997

48010.1 Policy

This document is the formal definition of the Department policy regarding the acquisition and use of workgroup computing technologies, including portable, stand-alone, and networked microcomputers, electronic mail, Internet and Intranet access, connectivity, and Web pages. It is CDC's policy that these technologies be used to:

- Increase employee and workgroup productivity.
- Enhance the sharing and distribution of departmental information, both within CDC and to external entities.
- Enhance overall departmental communication.
- Reduce the overall departmental operating costs by strategically deploying standard workgroup technologies at all levels of the organization.

48010.2 Purpose

The purpose of this policy is to establish standards and responsibilities for the acquisition, use, and management of workgroup computing within CDC. Specifically, the policy is intended to:

- Promote the identification of cost-effective opportunities for using workgroup computing technologies to support the accomplishment of the mission and program objectives within CDC.
- Ensure that the use of workgroup computing technologies is consistent with CDC's SISP, tactical plans, or other management plans.
- Ensure that existing CDC and State information technology infrastructure standards are met, and that individual workgroup computing activities do not preclude the implementation of other departmental applications on the same configuration.
- Establish policy structures, levels of approval, and accountability to define the appropriate use, acquisition, and support (maintenance and training) of workgroup computing technologies, including electronic mail functionality and Internet access.
- Ensure that the integrity and security of automated files, ITS, and program operations are not jeopardized by the use of workgroup computing activities, including connection to external networks (Internet).
- Establish acceptable use standards for departmental employees using workgroup computing technologies, including portable and desktop systems, electronic mail, and Intranet and Internet connectivity.
- Establish appropriate policy structures for departmental information that is electronically provided by CDC for public access by the Internet.
- Establish appropriate policy structures for the publication of departmental information that is electronically provided internally to CDC by the Intranet.

48010.3 Scope, Definitions, and Exclusions

This section defines the scope and definitions for the workgroup computing policy and the automated technologies that are excluded from this policy.

48010.3.1 Scope

The scope of this policy deals with the appropriate use, approval, and acquisition of off-the-shelf workgroup computing technologies within CDC to increase the productivity of individuals and groups of employees working in the same programmatic function. This policy is for the benefit of employees only and cannot be used to acquire equipment for the exclusive use of inmates.

A workgroup is a group of employees performing the same programmatic function. A programmatic function within CDC can be defined either by commonality of organizational structure or work objectives. For the purposes of this policy, accounting, personnel, and business services could each be considered a programmatic function. A correctional institution or parole region could also be considered a workgroup performing the same function, i.e. managing groups of inmates or parolees.

This policy supports the SAM 4989.1 which promotes the deployment of workgroup technologies to increase the overall efficiency of State organizations. The workgroup computing approach focuses on the deployment of proven "off-the-shelf" hardware and software systems and the interconnection of these systems. This policy also promotes the development and maintenance of consistent computer and network services and standards to ensure that life cycle support is minimized for all workgroup computing technologies.

The following are included as workgroup computing technologies:

- Commercial productivity software for such functions as word processing, spreadsheet analysis, time management, presentation graphics, Internet connection, remote communication access, workgroup file management, and electronic mail connectivity.
- Special purpose software applications, such as accounting or dietary management software, that are off-the-shelf productivity systems for an identified departmental workgroup.
- Portable and desktop systems based on microcomputer hardware and operating system.
- Full network server configurations to interconnect workgroup computing systems and provide standard electronic mail and Intranet capabilities.
- Necessary networks and communication devices to interconnect workgroup computing systems to facilitate internal and external communications and the sharing of information. The use of modems within CDC is limited to the requirements defined in DOM 48020, Departmental Modem Policy. While the acquisition of these devices can be considered part of a workgroup computing solution, additional levels of approval and justification within CDC organization are needed. Please see the referenced policy.

The policy and the processes that are defined herein are consistent with the overall strategic directions and tactical initiatives that exist in CDC for support of major program areas.

48010.3.2 Definitions

A glossary of terms has been provided in DOM 41010 EDP General Information. The list of terms conforms with the definitions of terms provided in the SAM 4989.1.

48010.3.3 Exclusions

SAM 4989.1 places limits on the applicability of the workgroup computing policy within a State organization. Any single workgroup computing request must be consistent with, and not exceed, the cost delegation level assigned to CDC, as stated in SAM 4819.34.

Any acquisition, maintenance, or support of workgroup computing requests that require a budget augmentation or that qualifies as an Advanced Technology Project, SAM 4821 through 4821.8, is not covered by the workgroup computing policy. However, it is permissible to use this policy to acquire equipment that is the normal workgroup complement of equipment (hardware and software) for new positions funded through a budgetary augmentation. More specifically, the policy **does not** apply to the following:

- Critical Applications. These are defined as acquired or developed applications that, if they were not available, even for short periods of time, would cause the State or CDC a significant negative impact regarding:
  - The health and safety of the public, State employees, or inmates.
  - The fiscal or legal integrity of State operations.
  - The continuation of essential departmental programs.
- Department Databases. These are systems that involve the creation and maintenance of files or databases that serve more than a single workgroup within CDC, or where a single workgroup constitutes CDC.
- Uploading of Data Files. Requests cannot include support applications involving the uploading of data to databases used by persons outside of the workgroup. Word processing, electronic mail, and Internet files are not considered data files for the purpose of this policy and as such are part of workgroup computing.
- Computer Programming. Acquiring computing technologies, where the proposed system is dependent on program design, coding, and ongoing programming support to develop and maintain the system, are not part of

workgroup computing. Both procedural languages used to create database applications, and compilers used to compile procedural language routines, are considered elements of computer programming and are excluded from this policy. The creation of macros within a productivity software system and/or simple program instructions to run file management reports and queries as part of or by additional software packages, are **not** considered computer programming and can be part of a workgroup computing solution. The use of file management products, to manage information limited to a single workgroup, is allowed under this policy, so long as the file management functions are done through the use of menus and other pre-designed tools provided with the software package.

- Terminal Emulation. Acquiring computing technologies, for the sole purpose of emulating or replacing a computer terminal does not qualify as workgroup computing. While the use of microcomputer systems in a terminal emulation mode is not prohibited, such use alone does not constitute justification for acquisition of microcomputer commodities.
- Specialized or Single-Purpose Systems. Acquiring specialized, single-purpose desktop configurations, such as computer-aided design systems, desktop publishing systems, programmer workbench systems, or artificial intelligence systems does not qualify as workgroup computing. However, software-based applications on a general purpose personal computer may be covered by the workgroup computing policy. For example, desktop publishing employing word processing, graphics, and page layout software packages on a general purpose personal computer falls within this policy. Desktop publishing employing a specialized computer system that has been developed and marketed for the sole purpose of doing desktop publishing, does not.

Units wishing to initiate information technology projects that are not covered by the workgroup computing policy shall follow the procedures for planning and justifying such projects as specified in SAM 4819.3 through 4819.39.

48010.4 Responsibilities

The various areas of responsibility under the workgroup computing policy are summarized in the following sections.

48010.4.1 Department Management

As defined in the SAM 4841.1, the Director has ultimate responsibility for information technology, security, and risk management. The Director has the ability to delegate by policy, procedure, or written notification these responsibilities to other individuals in CDC. The specific requirements for the Director or his designee are to ensure that CDC has:

- A current information management strategy and a current or planned information technology infrastructure description on file, and that the workgroups computing acquisitions and usage are consistent with these strategies.
- Processes to safeguard workgroup computing systems and the information generated and transmitted by these systems.
- The necessary policies and procedures for the technical network support activities, including installation, configuration, problem-determination, maintenance, backup, recovery, and all other activities, which would be in addition to those normally associated with stand-alone personal computers.
- The necessary policies and procedures to provide support and services for access to the Internet, Intranet, and electronic mail systems and servers including installation, configuration, problem-determination, maintenance, backup, recovery, security, and all other activities, which would be in addition to those normally associated with networks and communication systems.

The method in which the Director of CDC will ensure compliance with these responsibilities, is summarized in the remainder of this section.

48010.4.2 Assistant Director of Communications

The Assistant Director of Communications within CDC has responsibility for developing policies, guidelines, and procedures to ensure the appropriate disclosure and protection of departmental information when being transmitted outside and/or accessed from outside of the organization. Since one of the primary purposes of workgroup computing is to improve the method of electronic communication, the Assistant Director of Communications, by delegation of the Director, is responsible for ensuring that the workgroup computing policy conforms with departmental communication policies.

Responsibilities of the Assistant Director of Communications:

- Develop and maintain standards for Internet Web pages within CDC to define the "look, feel, and content" of such pages. This scope does not include Intranet Home page standards or Intranet/Internet Web sites.
- Review and comment on all workgroup policies and procedures that allow for the electronic distribution of departmental information outside of the organization using workgroup computing technologies. (Approved information technology projects do not fall under these policies.)
- Provide assistance in the development of departmental training materials to ensure that users understand their responsibilities as they pertain to the electronic transmittal of information using workgroup computing technologies.
- Ensure that auditing and record keeping standards are not in conflict with the IPA monitored by the Assistant Director of Communications.

48010.4.3 Information Security Officer

The Information Security Officer within CDC has responsibility for developing policies, guidelines, and procedures to ensure the appropriate security and safety of information technology resources, including the systems and resident information. Since one of the primary purposes of workgroup computing is to improve the process for information distribution and communication both internal and external to the organization, the Information Security Officer by delegation of the Director, is responsible for ensuring that the workgroup computing policy is in conformance with departmental information security policies.

Responsibilities of the Information Security Officer:

- Review workgroup computing processes and request forms, CDC Form 1855, Workgroup Computing Justification, CDC Form 1855 B, Workgroup Computing Justification - Additional Modem Justification, and CDC Form 1856, Web Page Justification, to ensure that employees are given notification of security and auditing requirements and that security processes are being followed.
- Review and comment on workgroup policies and procedures that allow for the electronic access, retrieval, and storage of information on departmental workgroup computing systems to ensure that security requirements are being met.
- Provide assistance in the development of departmental training materials to ensure that employees understand their responsibilities as they pertain to the security of departmental information technology resources and information.

48010.4.4 ITS Management

The overall responsibility for the deployment and maintenance of information technology systems rests with ISD of the EC&ISD within the Support Services area of CDC. The ISD is responsible for the development and maintenance of CDC standards for workgroup computing technologies, with the exception of Internet Web page format and content, and the activities assigned to the Information Security Officer.

The ISD is responsible for the maintenance of the departmental networks, including the support of the infrastructure that interconnects departmental locations and provides remote access and connection to external entities. The ISD Data Center maintains the standards for CDC's Intranet and Internet Web site and for the "look-and-feel" of departmental Intranet Home pages. Intranet or Internet Web pages developed by the users will be implemented on the Intranet or Internet Web servers by ISD staff. Intranet access and electronic mail systems are provided as part of the standard department network infrastructure and are included in the standards for all new network installations that will connect to the ISD departmental network.

Within this framework, ISD is integrally involved in workgroup computing to develop policies and procedures regarding the acquisition, use, and distribution of information. The ISD's Data Center staff determines the information technology standards for hardware and software and provides the ongoing maintenance and support of the infrastructure and CDC's Intranet and Internet access capabilities. The Workgroup Computing Coordinator, who administers the processes to support workgroup computing, is also part of ISD. The ISD also provides the technical expertise in terms of software systems and networking to implement the various workgroup computing requests and provides assistance in the initial configuration and deployment of a full workgroup computing solution.

48010.4.5 Departmental Workgroup Computing Coordination

Responsibility for workgroup computing coordination within CDC is assigned to the ISD, which maintain three primary functions to support workgroup computing:

- Workgroup computing information dissemination and acquisition support.

- Provide general technical and networking expertise and assistance.
- Maintain the departmental network, including the infrastructure, hardware and communication devices, Internet access services, Intranet connectivity, and electronic mail.

The Workgroup Computing Coordinator will perform the dissemination of information, oversight of acquisition activities, and maintenance of standards lists. Responsibility for technical assistance and review of workgroup computing configurations will be assigned to the Data Center, including approval of new network installations and remote access authorization, maintenance of the departmental network, Internet Web site, and Intranet and electronic mail capabilities. Technical assistance for individual workgroup computing requests can also be provided based on the specific requirements of the request.

Responsibilities of ISD's workgroup computing coordination function are:

- Assist departmental management and individual departmental employees in the identification of opportunities for employing workgroup computing to improve personal and workgroup productivity.
- Provide overall interconnection of CDC using networks, remote access, and the Internet and Intranet by maintaining standards and offering set services as part of the departmental network.
- Assist in the justification of workgroup computing configurations, the specification of microcomputer and network commodities for workgroup computing, and the preparation of required documents.
- Coordinate the creation and maintenance of lists of CDC approved standard workgroup computing technologies.
- Review and approve individual workgroup computing technology acquisition requests.
- Assist in determining whether a workgroup computing configuration could support a proposed application in addition to its workgroup computing work.
- Maintain continuing liaison with departmental management to ensure that proposed workgroup computing implementations are:
  - Consistent with CDC's established strategy for information management. as described in CDC's SISP.
  - Preventing duplication of existing capabilities.
  - Not precluding the implementation of other departmental applications on the same configuration.
- Maintain the departmental network, Intranet and Internet Web sites, and access.
- Provide for backup procedures and disaster recovery processes that should be part of workgroup computing requests.

48010.4.6 Parole Automation Systems Unit, Institution, and Unit Computing Coordination

Responsibility for workgroup computing coordination within an institution or other departmental unit is assigned to the Computing Coordinator, usually an AISA. These coordinators perform key functions to support workgroup computing within their specific unit or institution. The Parole Automation Systems Unit performs these functions for P&CSD staff. The Computing Coordinators and Parole Automation Systems Unit assist with information dissemination and acquisition support and interface with ISD on workgroup computing requests. They also provide technical assistance and review workgroup computing configurations within their respective organizations. Additional technical assistance from ISD can also be provided based on the specific requirements of a workgroup computing request.

General responsibilities of the Computing Coordinators are:

- Assist institutions, unit management, and individual departmental employees in the identification of opportunities for employing workgroup computing to improve personal and workgroup productivity.
- Assist in the justification of workgroup computing configurations, the specification of microcomputer commodities for workgroup computing, and the preparation of required documents.
- Coordinate, review, and approve individual workgroup computing technology acquisitions.
- Assist in determining whether a workgroup computing configuration could support a proposed application in addition to its workgroup computing work.
- Maintain continuing liaison with CDC's ISD staff to ensure that proposed workgroup computing implementations are:
  - Consistent with CDC's established strategy for information management.
  - Preventing duplication of existing capabilities.
  - Not precluding the implementation of other departmental applications on the same configuration.

48010.4.7 Unit Supervisors

Unit supervisors are responsible for the work performed within their organization. This responsibility includes the access, use, and security of workgroup computing technologies and associated information. Workgroup computing technologies are considered a departmental resource and are assigned to staff based on justified need.

Responsibilities of the unit supervisor:

- Actively initiate and deploy workgroup computing technologies to improve the productivity and efficiency of their unit.
- Develop, review, and approve justifications for procurement of workgroup computing resources.
- Review and approve justifications for access to the Internet for purposes of information collection and communication external to CDC.
- Review and approve justifications to establish a Web site on either the Internet or Intranet for the distribution of departmental information, both internal and external to CDC.
- Supervise and approve the creation and updating of the content and format of Intranet or Internet Web pages.
- Ensure that all employees are trained in and aware of their responsibilities when using workgroup computing technologies, and that each employee has in their official personnel file a signed CDC Form 1857, Computing Technology Use Agreement.
- Ensure that employees use workgroup computing resources solely for assigned departmental activities appropriate to that workgroup.
- Initiate disciplinary action for employees who are inappropriately using workgroup computing technologies, up to and including termination of employment.

48010.4.8 Procurement

During the acquisition of workgroup computing technologies, a procurement process will follow and/or parallel the workgroup computing authorization process.

Responsibilities of Procurement:

- The necessary procurement documents are completed and the acquisition is completed in conformance with the PCC and departmental policies and procedures.
- Information technologies procurements have been authorized. For workgroup computing technologies, this means ensuring that the Workgroup Computing Coordinator has an approved CDC Form 1855 on file, and that the procurement documents have appropriately referenced this Form.

48010.4.9 Users

In an environment that encourages workgroups to make use of computing technologies to increase work efficiency and performance, the users become responsible for more than just a computer on their desk. They are members of a wider community of interdependent users and need to be respectful of other departmental users and safeguard the information that might be shared on these systems.

Responsibilities of Users:

- Understand and follow the acceptable usage guidelines for workgroup computing resources listed in DOM 48010.5.
- Seek guidance in areas for which policy and procedural clarification is needed.
- Participate in necessary training to further ensure the productive use of workgroup computing tools.

48010.5 Acceptable Uses and Ethics

The effectiveness of the departmental computing environment and shared information resources depends on the responsible behavior of all authorized users, managers, and administrators of these resources. Along these lines, guidelines are used to determine acceptable uses.

The CDC reserves the right to monitor and/or log all network activity, including electronic mail, with or without transaction-by-transaction notification, and therefore, users should have no expectation of privacy in the use of these resources.

Uses that are acceptable and encouraged for workgroup computing include and are limited to the:

- Performance of assigned departmental activities.
- Preparation, communication, and exchange of information directly related to the mission and work tasks of CDC or its workgroups.
- Announcement of laws, procedures, hearings, policies, and services or activities related to CDC.
- Professional society activities authorized by CDC.
- Administration of contracts or federal grants for departmental programs.
- Communication and exchange of information for professional development and to debate issues related to assigned governmental activities.
- Research and development of documents, reports, and analyses of information related to the departmental workgroup activities.

Workgroup computing technologies, including access to the Internet, should not be used to publish, display, or transmit any information that will:

- Violate or infringe on the rights of any other persons, including the right of privacy.
- Contain defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually-oriented, threatening, racially offensive or other biased, discriminatory material.
- Violate departmental policies and regulations prohibiting sexual harassment.
- Restrict or inhibit other users from using the system or the efficiency of the computing systems.
- Encourage the use of controlled substances or use of the system for the purpose of criminal intent.
- Violate State or Federal laws.

The CDC's policy is that users will not use the facilities and capabilities of workgroup computing to:

- Conduct activities not related to the mission or work tasks of the workgroup or CDC.
- Solicit the performance of any activity that is prohibited by law.
- Transmit material, information, or software in violation of departmental communication policies, or local, State, or federal law.
- Conduct any electioneering or political activities.
- Perform non-government related fund raising or public relations activities.
- Engage in any activity for personal gain or for personal business transactions.
- Make unauthorized purchases.

48010.6 Approved Technologies

It is the policy of CDC that standard configurations for workgroup technologies will be implemented to ensure a consistent approach for implementation, training, and support of these technologies. The Workgroup Computing Coordinator within CDC develops and maintains lists of departmental-approved, standard workgroup computing technologies. These standards are for microcomputer hardware and software systems, off-the-shelf special purpose applications, communication interconnectivity, including remote access to department systems and networks, and use of the Intranet and Internet.

These standards are developed to ensure consistency within the overall Department. Items on the technology standards lists have been selected because they are of proven capability and reliability, are appropriately priced, and are compatible with configurations already in use in CDC or in other State agencies. Minimum standards and lists will be updated in response to changing technology and State experience. Consideration is given to new categories of hardware and software based on the probability that a solution will be employed in more than one workgroup, and to maintain uniformity in the deployment of technology.

As part of CDC's network maintained by ISD, standard functionality is provided to departmental employees. Some of these features include virus check, Intranet access, print services, and electronic mail. Items that are provided as part of CDC's network **do not** require a workgroup computing request unless a new microcomputer is part of the request. Requests for new networks will be considered part of the overall departmental network and must meet the departmental network standards, including offering standard functionality.

In addition to the standard lists maintained by the Workgroup Computing Coordinator, ISD maintains the standards for network infrastructures, including Local Area Network's, Wide Area Network's, and Internet/Intranet connections. To ensure network interoperability and consistency within CDC, ISD's networking group will review and approve requests that involve new network installations, Internet access requests, Intranet Web pages, and exceptions to departmental standards.

Units proposing to acquire workgroup computing commodities are expected to select from these lists whenever possible. Proposals to acquire items not included in the lists will fall into one of two classifications:

- Requested technology falls into one of the standard categories defined by the ISD, and the Unit is requesting an "exception" to the standards in that category.
- Requested technology does not fall into one of the standard categories defined by the ISD and must be reviewed to ensure that the solution meets all of the requirements for being a workgroup computing technology. For example, a system to manage the planning of the dietary program in an institution could fall under the workgroup computing policy.

The first type of request will require, at a minimum, the approval of the Chief of Information Systems and must be based on a sound, justifiable business need. Rejected requests may be appealed through CDC's chain of command.

The second type of request must be approved by the departmental division office responsible for the specific workgroup computing request. The request must also be reviewed by the Workgroup Computing Coordinator on a case-by-case basis to determine if the solution falls within the parameters of a workgroup computing solution. Solutions that are in question may require an individual review by the control agency, as stated in SAM 4989.1. Requests that are deemed to meet the workgroup computing requirements will then be reviewed to determine if the proposed solution should be added to a departmental standards list.

48010.7 Development of Software

It is the policy of CDC to use commercial software packages for workgroup computing whenever possible, rather than undertake independent software development. Fully tested and documented commercial packages are readily available for most functions and are usually much less costly than custom-developed programs.

Computer programming **does not** fall within this workgroup computing policy and shall be justified in accordance with the requirements of SAM 4819.3 through 4819.39 and DOM 43020.

48010.8 Acquisition Authorization Process

For the purposes of this policy *acquire* refers to either the procurement of and/or receiving approval to utilize workgroup computing technologies. As such, there are two processes necessary for CDC to acquire workgroup computing technologies. The first is the authorization and approval process and the second is the procurement process. The procurement process for workgroup computing technologies falls under CDC's procurement policies and procedures which are defined in DOM Chapter 20000, Financial Operations, Subchapter 22000, Budget Administration, and Chapter 40000, MIS, and Subchapter 45000, General Procurement and Contracting.

Each procurement of a workgroup computing technology, is subject to management review and approval before an actual order can be placed or the unit takes possession of the equipment or software. Approval is required to gain Internet access or to establish an Internet or Intranet Web page.

The approval process consists of:

- Determining the hardware, software, and network requirements.
- Completing the CDC Form 1855, CDC Form 1855 B, CDC Form 1856, and/or CDC Form 1857.
- Routing the CDC Form 1855 and documents for approvals and signatures.
- Getting necessary reviews and approvals for acquisitions that will involve: new network installations, new systems that will distribute or access departmental information, and exceptions to workgroup computing standards.
- Getting necessary review and approvals to establish Internet or Intranet Web page or to gain Internet browsing access.

48010.8.1 Justification

Unit management is responsible for performing the needs assessment and for preparing the justification associated with the proposed approval or acquisition of workgroup computing commodities. This process shall be documented using the CDC Form 1855, CDC Form 1855 B, and/or the CDC Form 1856. The CDC Form 1855 is used to justify the acquisition of workgroup computing technologies. The form is also used to request and gain approval for Internet browsing access. The CDC Form 1856 is used to justify establishment of Web or Home pages. These activities shall also be in conformance with the applicable sections of SAM.

The amount of information and degree of detail provided shall be commensurate with the nature, complexity, risk, and expected cost of the proposed workgroup computing effort. When such applications include the use of networks or Internet access using "servers" or other shared devices, unit management must include consideration and justification for the necessary technical support for activities such as installation, configuration, problem-determination, maintenance, backup, recovery, and all other activities that would be in addition to those normally associated with stand-alone personal computers.

48010.8.2 Forms

The basis for the workgroup computing justification is the CDC Form 1855, which is maintained by the Workgroup Computing Coordinator and is modeled after the form shown in SAM 4991. This form is updated on a periodic basis and is modified to support specific processes that are unique within CDC. The form provides for the acquisition of portable and desktop hardware and software and Internet access. It also provides for necessary approval signatures and certifications. This form will be available through Electronic Distribution on the CDC Intranet.

The CDC Form 1856 is used to request establishment and maintenance of an Internet Web page for distribution of information outside CDC, or an Intranet Home page for distribution of information internal to CDC. Form maintenance is coordinated by the Workgroup Computing Coordinator with input from the Assistant Director of Communications and the Data Center. This form is updated on a periodic basis and is modified to support specific processes that are unique within CDC. The form requesting approval to create a home page needs to be accompanied by a CDC Form 1855 when a Web site will be established requiring the acquisition of hardware, software, and/or communication devices. This form will be available through Electronic Distribution on the CDC Intranet.

The CDC Form 1857, must be on file for each employee using workgroup computing technologies, accessing departmental networks, and/or accessing the Internet. This form notifies the users of their responsibilities as they pertain to using these technologies; it also notifies them that the information maintained and distributed by the user is not considered "private." It is the policy of CDC that each new employee completes the CDC Form 1857 as part of their employee orientation process. The CDC Form 1857 should be maintained in the employee's official personnel file. If a CDC Form1857 is not currently on file when workgroup computing technologies are being requested for an employee, then the Unit Supervisor should have the employee sign the Form and have it filed in the official personnel file. This form does not get routed to the Workgroup Computing Coordinator.

48010.8.3 Unit Approvals

Each request for acquisition of workgroup computing technology is subject to management review and approval before the order can be placed or the unit takes possession of the equipment or software. Once the request has been completed there are three basic levels of review: unit management, institutional or divisional review, and ISD review. The Deputy Director may delegate approval of workgroup computing requests within each division. However, at a minimum, at least one level of management above the unit management must review, and approve each workgroup computing request prior to submitting the request to ISD. If the first level manager is an Assistant Director or Assistant Deputy Director, then this level of approval is sufficient for the workgroup computing justification process.

For workgroups within institutions other than Health Care Services, the following minimum approvals are needed for the CDC Form 1855:

- Unit Supervisor.
- Institution Computing Coordinator.
- Warden, or his/her designee.

For workgroups within P&CSD**,** the following minimum approvals are needed for the CDC Form 1855:

- RPA.
- P&CSD Computing Coordinator.
- Deputy Director or his/her designee.

For workgroups within Health Care Service Division units that are co-located within an institution, the following minimum approvals are needed for the CDC Form 1855:

- Unit Supervisor (local and/or headquarters).
- CMO.
- Institution Computing Coordinator.

For workgroups within headquarters organizational units, the following minimum approvals are needed for the CDC Form 1855:

- Unit Supervisor.
- Deputy Director or his/her designee.

Acquisition of additional workgroup computing capabilities for previously acquired configurations are subject to similar reviews and approvals. Requests for Internet access will be processed in the same manner as acquiring other workgroup computing technologies, with the same approvals. Internet and Intranet Web page requests will also follow the approval process as shown above.

Additional approvals are needed for exceptions to standards, new network installations, Internet access, remote access to the departmental systems and network and/or modem usage. These additional levels of approval have been defined in the appropriate sections of this policy.

48010.8.4 Routing and Final Approvals

Once the workgroup computing analysis and the justification documents are completed with departmental certifications and signatures as per DOM 48010.8.2, the forms should be routed as follows:

- CDC Form 1855: The completed form should be forwarded to the Workgroup Computing Coordinator for final approval and processing. The purpose of the review and approval is to ensure that the proposed request conforms to policy and is consistent with departmental standards. The coordinator will route the request for other necessary technical and security reviews and certifications. If the request for workgroup computing commodities include remote access requirements, network products, or Internet access, the procurement documents shall be further reviewed by the Data Center to determine:
  - Technical specifications are consistent with both the proposed use and CDC's strategic direction and established standards.
  - Adequate level of technical network support is addressed in the CDC Form 1855.
- CDC Form 1856: Standard Internet/Intranet Web page requests should be routed to the Data Center for approval. The Data Center will then forward these to the Workgroup Computing Coordinator for retention. If an Internet Web page is not in conformance with departmental Web page standards and/or if this is the initial request for public distribution of departmental information as per applicable departmental communication policies, the request should be routed to the Assistant Director of Communications for approval.

If the request for workgroup computing technologies involves the installation of a new network or external department network connections within a facility that is not in conformance with departmental standards, the unit management may be required to complete an additional risk analysis to be reviewed by CDC's Information Security Officer before the request is routed to procurement.

Copies of the documentation regarding the justification of workgroup computing technologies shall be maintained in CDC's files within ISD. The Workgroup Computing Coordinator will approve the acquisition documents related to workgroup computing requests.

48010.8.5 Post-Implementation Evaluation

Unit management shall complete the CDC Form 1855 A, Workgroup Computing Justification, Post-Implementation Evaluation, no later than six (6) months after installation of the workgroup computing configuration or product.

The purpose of the Post-Implementation Evaluation is to determine:

- The unit has realized the benefits projected at the time acquisition of the configuration was justified.
- Unanticipated problems have been associated with the use of the configuration and how those problems have been resolved.
- The configuration is being used in compliance with CDC and State policies.

A copy of each evaluation shall be submitted for review to the Workgroup Computing Coordinator who shall maintain it on file.

48010.9 Security

The use of workgroup computing within CDC shall be in accordance with all applicable provisions of the SAM 4840 through 4845, dealing with information security and risk management, and with the specific provisions of SAM 4989.7, dealing with security. Users of these configurations shall be knowledgeable about the SAM provisions as well as CDC's security and risk management policies associated with workgroup computing configurations as defined in DOM 49010 through 49030. The CDC staff must also be aware that computer viruses pose a potentially serious threat to departmental computer and information assets. Virus protection must be implemented on every departmental workstation.

The CDC will ensure that security precautions are in place for access to the Internet/Intranet and external electronic mail systems. Such safeguards include firewalls, anti-virus systems, password security, information encryption and other security measures to:

- Eliminate unauthorized access to departmental systems and information.
- Ensure that confidential or sensitive information is not improperly disclosed or distributed.

The ISD, Network Services Unit, is responsible for defining and/or maintaining the infrastructure for these security systems. The user is responsible for following the established processes that are defined. The Information Security Officer is responsible for reviewing the processes to ensure that they meet the departmental security policies and requirements.

48010.9.1 Confidential and Sensitive Information

The vast majority of information maintained by CDC is confidential and/or sensitive in nature. Its untimely or unauthorized release external to the organization may have significant, adverse impact on CDC.

The policies controlling the communication of departmental information external to the State organization is governed by DOM Chapter 10000, Subchapters 12000, 13000, and 14000. Information provided to the public by the Internet or other electronic transmittal methods external to CDC shall comply with all related DOM policies, laws, and State regulations regarding confidential or sensitive information.

Electronic mail that travels through the Internet could be intercepted. To eliminate this possibility, no confidential and/or sensitive information may be transmitted by electronic mail or other means over the Internet unless it is encrypted.

All questions regarding the distribution or access to confidential and sensitive information should be directed to the CDC's Assistant Director of Communications.

All proposals for using workgroup computing systems to maintain or access files containing confidential or sensitive information, as defined in SAM 4841.3, shall meet the standards set by CDC's Information Security Officer, or will be individually approved by the Information Security Officer, before implementation (SAM 4841.1). Conformance to information security standards or the individual request review, shall ensure that the request complies with all applicable provisions of the SAM 4840 through 4845 dealing with information security and risk management.

48010.9.2 Integrity of Information

Information maintained on workgroup computing configurations shall be subjected to the same degree of management control and verification of accuracy that is provided for information maintained in other automated and manual files within CDC, as defined in the appropriate sections of the DOM.

If a data file is downloaded to a workgroup computing configuration from another computer system, the requirements for information integrity and security that have been established for the data file shall be adhered to while it is stored at the workgroup level.

48010.9.3 System Backup

Provisions shall be made to safeguard against the loss of information and programs stored on workgroup computing configuration as a result of product failures or power failures. Copies of all data files and software shall be stored in a safe location. A regular schedule for making backup copies of all data files shall be established. Unit Supervisors shall ensure that backup procedures are carried out. Training in backup options and procedures shall be ensured by Unit Supervisors. The ISD and the Information Security Officer are responsible for setting guidelines and standards for backup procedures.

48010.10 Legal

Existing laws and legal renderings related to privacy, confidentially, and use of computers concerning information technology, especially in the areas of electronic access, e-mail privacy, and copyright protection must be complied with. Two primary laws are the Electronics Communication Privacy Act and the Comprehensive Computer Fraud and Abuse Act. It is CDC's workgroup computing policy to comply with these laws.

48010.10.1 Copyright Material and Licenses

Software license agreements shall be strictly adhered to. Proprietary software cannot be duplicated, modified, or used on more than one machine, except as expressly provided for in the manufacturer's license agreement program updates may be downloaded from the Internet in accordance with the owner's license agreement.

Public domain software, while available under the copyright laws to all individuals should not be downloaded to a departmental workgroup computing device unless it is part of the departmental standard as documented by the Workgroup Computing Coordinator and/or approved by the unit manager.

48010.10.2 Ownership of Resources

The CDC has determined that all workgroup computing technologies are the property of CDC, and that the use of these technologies, including the content of data files and electronic mail messages, is not considered private to the user.

It is CDC's requirement, based on the confidentiality and sensitivity of its business, to control access to and monitor that use of State-provided workgroup computing resources, including e-mail systems. The CDC will inform workgroup computing users regarding computer privacy in the following manner:

- As part of the workgroup computing request process by the CDC Form 1857.
- As part of the new employee orientation process.

This notification will be given in writing and the user must sign the notification form as part of the new employee orientation process or as part of the workgroup computing request process. It is CDC's policy that this form be made part of the employee's official personnel file.

48010.10.3 Regulation and Enforcement

The director and his designated representatives are responsible for ensuring compliance with provisions of this policy and for investigating suspected noncompliance. Service to a user may be suspended when deemed necessary for the operation and/or integrity of the departmental infrastructure or connected networks. User privileges, user accounts, and/or password access may be withdrawn without notice.

When an instance of noncompliance is suspected or discovered, CDC shall proceed in accordance with CCR (15) (3) 3413, Incompatible Activities, and CCR (2) (1) General Civil Service Rules. Internal discipline, up to and including discharge, may be appropriate in some cases of noncompliance with this policy. Criminal or civil action may be initiated in appropriate instances.

48010.11 Documentation

Complete documentation shall be maintained for all of the microcomputer commodities used for workgroup computing.

Documentation shall include:

- Equipment and Software. Manuals relating to the installation, maintenance, care, and use of equipment and proprietary software shall be maintained with the equipment or in a central library, as appropriate.
- Procedural Documentation. Each workgroup application that makes use of a proprietary software package (including database systems, spreadsheet software, or any software that maintains data files) shall have documentation sufficient to allow productive use of the application. In addition to standard user manuals, some documentation that may be needed could include:
  - Instructions containing the scope and purpose of the application.
  - Specific data entry and processing instructions for the application.
  - File descriptions including data dictionaries.
  - Lists of all utility programs and subroutines used by the application.
  - Sample report/screen formats for the application.

48010.12 Training

Workgroup management is responsible for ensuring that staff members possess the knowledge and skills necessary for effective use of workgroup computing facilities, and that there is sufficient depth of training to prevent disruption of key activities in the event of unexpected staff changes. At least two staff members should be trained in using each workgroup computing application and the equipment that it uses.

The Workgroup Computing Coordinator shall assist in the identification and scheduling of suitable training and in coordinating the development of training materials to be included as part of new employee orientations.

Users granted access to the Internet shall be required to abide by the acceptable use standards and shall have sufficient training in accordance with this and other policies related to electronic communications.

48010.13 Maintenance and Repair

The CDC shall make provisions for necessary routine maintenance, as well as for the repair of malfunctioning equipment. It is the responsibility of workgroup management to budget necessary funds for maintenance and to ensure that maintenance schedules are met.

48010.14 Inventory of Assets

The CDC shall maintain an inventory of its significant microcomputer commodities used for workgroup computing configurations. The inventory shall provide a description of each item (including serial and model numbers of equipment and version numbers of software), its date of acquisition, and the unit to which it is currently assigned. This inventory may be part of CDC's existing inventory system. The CDC shall also maintain inventories of licensed software and significant applications installed on workgroup computing configurations. These inventories will be available for audit purposes.

48010.15 Revisions

The Chief, ISD, or designee, shall be responsible for ensuring that the contents of this section are kept current and accurate.

48010.16 References

Comprehensive Computer Fraud and Abuse Act.

DOM §§ 10000, 20000, 40000, 12000, 13000, 14000, 41010, 43020, 48020, 43020, 49010, 49020, and 49030.

Electronics Communication Privacy Act

CC § 1798, et. seq. (Information Practice Act).

SAM § 4800 - 5901.

PCC.

ARTICLE 42 — DEPARTMENTAL MODEM POLICY*

Effective December 22, 1992

Not Cleared For Statewide Use

48020.1 Policy

The Department recognizes the potential for increasing the speed and flexibility in which files can be transferred electronically through the use of modems; however, this potential benefit shall be weighed against the inherent hazards of misuse in CDC facilities.

48020.2 Purpose

The general purpose of this policy is to establish standards for the use and management of modems within the Department's operations. This policy is to be used for the purchase of all modems, including those within and outside facilities.

Scope of the Modem Policy

SAM 4989.1 states that modem usage consistent with the Department's security and risk management policy are covered by the Department's personal computer policy, and therefore follow the normal supplemental equipment justification process. However, due to the potential for misuse, special security precautions need to be addressed when using modems within a facility, parole office, or wherever inmates or parolees may have access to a PC. Consequently, a special modem supplemental equipment request form shall be used when requesting the acquisition of a modem. This form requires additional information for those modems that are to be used within any situation where inmates or parolees may have access to a personal computer.

48020.3 Benefits of Modems

Department managers are encouraged to investigate the benefits of using modems with a personal computer. However, any potential benefit shall be weighed against the inherent security risks involved with modems.

48020.4 Responsibility for Modems When Used With Personal Computers in Department

Management Responsibility

Management responsibility for the use and security of each modem resides with the Warden of each individual facility or the Administrator of each parole office. Responsibility resides also with managers who are responsible for personnel who regularly use a computer with an attached modem. It is further suggested that each facility's AISA be involved in the acquisition and use of modems within the facility.

All modems are considered departmental resources. They may be assigned for the exclusive use of an individual or unit within the Department, but such assignment may be changed at any time. In order to maintain an accurate and current inventory of departmental modems, every change in physical location (even within a branch or facility) shall be reported to the MIS-SU, located in the OISB, so that the modem inventory list may be updated.

If a modem is transferred to a different location, the party from whom the modem is transferring must notify in writing, the appropriate property custodian. In headquarters, notify the property controller in the BSS. In the facilities, notify the property controller or Business Office. In the P&CSD, notify Parole Automation.

User Responsibility

Users of modems shall comply with State and CDC policies governing the use of modems with a personal computer.

The use of all CDC modems is restricted to official business of the Department. Unit supervisors or their designee have authority for modems under their control, and shall limit access to such modems to ensure their security at all times. It is recommended that a log be kept for each modem itemizing usage by date, transmitting user, start time, time signed off, software used, data transmitted, and line speed.

48020.5 Modem Acquisition Within CDC

Revised May 5, 1993

The acquisition of modems for use within the CDC shall be in compliance with the Department's personal computer and modem policies and the applicable sections of the PCC and SAM.

In addition, the following restrictions apply to modem use within facilities, parole offices, or any area that may be accessed by an inmate or parolee:

- There shall be no inmate or parolee access to a personal computer which have been approved for use of a modem.
- There shall be no inmate-developed programs on personal computers with modems.
- There shall be no inmate or parolee access to Local Area Networks containing modems.
- Modems shall not be purchased as part of a personal computer acquisition without complying with the Department's modem policy.
- Internal and pocket modems shall not be purchased or used within the facilities. In addition, internal and pocket modems shall not be purchased or used in regional parole offices or units unless the personal computer utilized is located and operated in a secure area which cannot be accessed by parolees. (internal modems may be installed in laptop personal computer assigned to headquarters and parole personnel as long as the equipment: (1) remains under the physical protection of designated personnel, (2) is locked in a secure area/vehicle when not in use, and (3) cannot be accessed by unauthorized users.
- Pocket modems used currently in the facilities shall be recalled and external modems substituted in their place.

48020.6 Modem Security Policy Within CDC

Each facility and parole office is to develop a policy to ensure the security of modems used within that facility or parole office. The policy shall include procedures to ensure that:

- All modems are safeguarded when in use and protected from unauthorized access when not in use. External modem procedures shall include a plan to physically lock external modems when not in use.
- The physical location of each modem is tracked at all times.
- An on-site evaluation of modem use is performed no later than 90 days after installation of each modem installed in a facility. This on-site evaluation shall be conducted by Institutions Division or P&CSD staff, respectively.

It is recommended that modems in facilities be used on dedicated data lines or a basic business line with call detail installed exclusively for modem communications. It is also suggested that an analysis be conducted to assess which type of communications service is more cost-effective to the user. By

assessing the length of time involved in the actual transmission of data and the distance and speed (baud rate) of the transmission, it can be determined which service is most appropriate to use.

48020.7 User Training on Effective Modem Use

Unit management is responsible for ensuring that staff members using modems possess the knowledge and skills necessary for effective modem usage. Such staff shall be trained sufficiently (e.g., outside vendors, State EDP training) so as to maximize the effective use and protection of CDC modems.

48020.8 Revisions

Revised May 5, 1993

The Deputy Director, ASD, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

48020.9 References

SAM § 4989.

ARTICLE 43 - HANDHELD COMPUTING DEVICES

May 26, 2006

48050.1 Policy

It is the policy of the California Department of Corrections and Rehabilitation (CDCR) to utilize handheld computing devices, such as BlackBerries and Treos, in a manner that is safe, efficient, and cost-effective. BlackBerries and Treos are handheld devices that operate as a cellular telephone, Personal Digital Assistant (PDA), and allow Internet/e-mail capability.

48050.2 Purpose

The purpose of this Policy is to ensure that use of handheld computing devices complies with approved information security practices, does not endanger the users or the safety of the facilities within the Department, and that the devices are procured in the most cost effective manner in keeping with the Department's Desktop and Mobile Computing Policy.

48050.3 Definitions

Computer Security

The technological safeguards and managerial procedures that can be applied to computer hardware, programs, data, and facilities to ensure the availability, integrity, and confidentiality of computer-based resources.

E-mail

Written communication transmitted electronically using computers or handheld computing devices connected to the network(s) or via wireless transmission, such as BlackBerries.

Handheld Computer

Synonym for PDA.

Information Assets

Any documents, electronic files, or records that contain or are used to process, manage, or store information necessary to the operation of the CDCR.

Information Security

The protection of automated information against unauthorized access (accidental or intentional), modification, destruction, or disclosure.

Personal Digital Assistant (PDA)

Palm-sized computer that can sync with a workstation and allow the user to refer to information on the workstation without having to print it. Schedules, e-mails, documents, and spreadsheets, as well as dictionaries and phone lists, can be stored and accessed as needed.

Risk

In the context of information systems, the likelihood or probability that a loss of information assets or beach of security will occur.

Wireless

Communications transmitted without wires, such as radio, microwave, or infrared.

48050.4 Responsibilities

It is the responsibility of the Wardens, Superintendents, Associate Directors, Assistant Secretaries, and Regional Administrators and their designees to approve the purchase for the handheld devices using the process outlined in Department Operations Manual (DOM), Chapter 4, Article 41, Section 48010.1. The CDC Form 1855 will be utilized to document a brief summary of the request, the justification of need, the amount of support needed to maintain the device, and the necessary approval signatures. Approval documentation shall be forwarded to the Desktop and Mobile Equipment Coordinator, Enterprise Information Systems (EIS), for final processing.

Each Division Director is responsible for reviewing the monthly usage statements to ensure employees are not exceeding the allocated minutes under the terms of the contract in accordance with DOM Chapter 1, Article 12, and the relevant sections of the Youth Authority Manual (YAM).

It is the responsibility of the Chief Information Officer, Office of Information Technology, to maintain a user's guide that would outline the purpose, features, and associated costs for handheld devices. This document, named "A Practical Guide to Handheld Computing Devices," will be available via the Department's intranet site. The user guide will be updated at a minimum of every six months or as needed.

It is the responsibility of the Information Security Officer (ISO) to oversee Department policy and procedures to protect it's information assets, including confidential and sensitive information, e-mails, and documents found on handheld computing devices. The ISO will develop a risk assessment and mitigation program.

Additionally, there is a responsibility by all persons using handheld devices to do so in a manner consistent with the information security practices outlined in DOM Chapter 4, Article 45, and the relevant sections of the YAM.

48050.5 Authorized Use

Handheld computing devises, such as BlackBerries and Treos, will be issued using the same guidelines outlined in the DOM for cellular telephones, as set forth in DOM Chapter 1, Article 12, Section 12070.18. Such devices will also be issued and managed in accordance with any applicable sections of the YAM.

The following staff is authorized to use Handheld Computing Devices:

- Any personnel required to be available to the Governor's office on an as-needed and immediate basis, via email, including but not limited to:
  - Secretary
  - Undersecretary
  - Chief Deputy Secretaries
  - General Counsel
  - Legislative Liaison
  - Office of Public and Employee Communication
- Any person designated by the CDCR Secretary or Undersecretary as being required to be available on an as needed and immediate basis, via email, including but not limited to:
  - Division Directors and Executive Staff
  - Assistant Secretaries
  - Wardens
  - Chief Deputy Wardens
  - Chief Deputy General Counsel
  - Health Care Managers
  - Director, Juvenile Facilities
  - Assistant Director, Juvenile Facilities
  - Assistant General Counsels
  - Superintendents
  - Regional Parole Administrators
  - Deputy Regional Administrators
- Any personnel required to be remote to their home office on a regular or extended period (typically greater than 50% of each day) and requiring e-mail to do their job, including but not limited to:
  - Information Technology support staff
  - Auditors
  - Staff Counsels

48050.7 Revisions

The Chief, EIS, or designee, shall be responsible for ensuring that the contents of this Article are kept current and accurate.

48050.8 References

DOM §§ 12070, 48010, and 49020.

YAM.

ARTICLE 44 — GENERAL INFORMATION

Effective November 30, 1992

49010.1 Policy

It is the policy of the Department to protect against the unauthorized modification, deletion, or disclosure of information included in the Department's automated files and data bases. Such disclosure might compromise the integrity of Department programs or violate individual rights to privacy, and may constitute a criminal act. The Department regards its information assets, including data processing capabilities and automated files, to be essential public resources. Many aspects of the Department's operations would effectively cease in the absence of critical computer systems, including automated systems necessary for the protection and safety of persons in the custody of the Department. Accordingly, the Department shall assume full responsibility for the proper classification, use, and protection of its automated information. Further, each element of the Department that employs information technology shall establish risk management and disaster recovery planning processes for identifying, assessing, and responding to the risks associated with its information assets.

49010.2 Purpose

The purpose of this policy is to establish and maintain a standard of due care to prevent misuse or loss of Department information assets. This policy establishes internal policies and procedures that:

- Establish and maintain management and staff accountability for the protection of departmental information assets.
- Establish and maintain processes for the analysis of risks associated with departmental information assets.
- Establish and maintain cost-effective risk management processes intended to preserve the Department's ability to meet program objectives in the event of the unavailability, loss, or misuse of information assets.
- Protect departmental employees who are authorized to access the Department's information assets from temptation, coercion, and threat.

49010.3 Information Assets Applicability Within the Department

Information assets covered by this section include: (1) all categories of automated information including, but not limited to, records, files and data bases; and (2) information technology facilities, software, and equipment (including personal computer systems) owned or leased by CDC.

49010.4 Statutory References Concerning the Confidentiality and Security of Information Within CDC

GC 1171 requires the director of each department that uses, receives or provides data processing services to designate an Information Security Officer (ISO) who shall be responsible for implementing State policies and standards regarding the confidentiality and security of information within the Department. These policies and standards shall include, but are not limited to, strict controls to prevent unauthorized access of: data maintained in computer files, program documentation, data processing systems, data files, and data processing equipment located physically in the Department.

The primary provisions affecting the classification and dissemination of information under the control of California State agencies is found in the State Constitution, in statutes, and in administrative policies:

- Article 1, Section 1, of the Constitution of the State of California defines pursuing and obtaining privacy as an inalienable right.
- The IPA of 1977 (CC 1798, et seq.), places specific requirements on State agencies in the collection, use, maintenance, and dissemination of information relating to individuals.
- The PRA (GC 6250-6265), provides for the inspection of public records.
- The State Records Management Act (GC 14740-14770), provides for the application of management methods to create, use, maintain, retain, preserve, and dispose of State records, including the determination of records essential to the continuation of State government in the event of a major disaster. SAM 1601 through 1699 contain administrative policies to implement provisions of this law.
- The California Computer Crime Statute (Calif. Rev. Stat 1987, Sect. 502, Ch 1499, 1 January 1988) covers five offenses:
  - Manipulating data, a computer system, or computer network to devise or execute a fraud.
  - Knowingly accessing and without permission taking copies or using any data from a computer or taking any supporting documentation, internal or external, to a computer.
  - Theft of computer services.
  - Knowingly accessing and without permission damaging data, computer software, or computer programs, internal or external, to a computer.
  - Disrupting or denying computer services to an authorized user.
- The Federal Copyright Act of 1976, provides for the prosecution of persons guilty of the theft of computer programs.

49010.5 Exemptions From Information Systems Security Policy

Exemptions to this policy may be granted by the Management Information Systems Committee. The decision to grant an exemption shall be based primarily upon a risk analysis submitted to the Committee and the recommendation of the CDC ISO.

49010.6 Information Management Annual Plan Reporting Requirements

The Information Management Annual Plan (IMAP), submitted by the Department to the DOF, Office of Information Technology (OIT), shall contain a certification that the Department is in compliance with State requirements concerning information technology security and risk management. This certification is signed by the CDC Director. In addition, the IMAP shall provide the name, title, business address and telephone number of the agency's ISO.

49100.6.1 Operational Recovery Plan Reporting Requirements

The Department shall file an information copy of its Operation Recovery Plan (ORP) with OIT by January 31 each year. A copy of the ORP shall be provided to the Teale Data Center.

49010.6.2 Incident Reporting Requirements

It is the responsibility of all departmental employees to report all incidents that would place the Department's information assets at risk. It is the policy of the Department that the following incidents shall be reported through the chain of command to the departmental ISO:

- Any incidents involving unauthorized access to automated data, automated files, or data bases.
- Any incident involving the unauthorized modification, destruction or loss of automated data, automated files, or data bases.
- Any incident involving a virus, worm, or other such computer contaminant (see also DOM 41010).
- Any incident involving the unauthorized use of computer equipment, automated data, automated files, or data bases.
- Any incident involving the misuse of the information assets of the Department.

49010.6.3 Incident Report Format

The following information concerning each incident shall be reported to the departmental ISO within five working days of any awareness of the occurrence of the incident:

- Date of the incident.
- Contact person.
- Description of the incident and whether it is a major incident as described in DOM 49040.36.

49010.6.4 Incident Investigation

Department management shall investigate promptly all reported incidents as defined in DOM 49010.6.3.

The CDC ISO shall investigate each such reported incident to determine the facts and to prepare a report. The report shall have a section that contains a report of the incident prepared by the appropriate local management.

49010.6.5 Information Security Incident Report To DOF

A report of major incidents as illustrated in SAM 4845 shall be submitted to OIT within ten working days of the Department's first awareness of an incident involving one or more of the following:

- Unauthorized intentional release, modification, or destruction of confidential or sensitive information, or the theft of such information including information stolen in conjunction with the theft of a computer or data storage device.
- Use of a State information asset in the commission of a crime.

- Intentional damage or destruction of State information assets, or the theft of such assets with an estimated value in excess of $500.

The report shall be signed by the Department Director and the Department ISO.

49010.7 Revisions

Revised April 16, 1993

The Chief, ISD, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

49010.8 References

Revised April 16, 1993

Federal Copyright Act of 1976.

Article 1, § 1 of the Constitution of the State of California.

California Computer Crime Statute (Calif. Rev. Stat 1987, §. 502, Ch 1499, 1 January 1988)

IPA of 1977.

PRA.

GC §§ 1171, 6250 - 6265, and 14740 - 14770

SAM §§ 1601 - 1699, and 4845.

DOM §§ 41010 and 49040.

ARTICLE 45 — INFORMATION SECURITY*

Revised December 5, 2003

49020.1 Policy

It is the policy of the California Department of Corrections and Rehabilitation (CDCR) to protect against the unauthorized modification, deletion, or disclosure of information included in agency files and databases. The Department regards its information assets, including data processing capabilities and automated files, to be essential resources. The Department shall assume full responsibility for ensuring the security and integrity of its automated information.

49020.2 Purpose

The purpose of this Policy is to establish and maintain a standard of due care to prevent misuse or loss of Department information assets. This policy establishes internal policies and procedures that:

- Establish and maintain management and staff accountability for the protection of departmental information assets.
- Establish and maintain processes for the analysis of risks associated with departmental information assets.
- Establish and maintain cost-effective risk management processes intended to preserve the Department's ability to meet program objectives in the event of the unavailability, loss, or misuse of information assets.
- Protect departmental employees who are authorized to access the Department's information assets from temptation, coercion, and threat.

49020.3 Statutory References Concerning the Confidentiality and Security of Information within CDCR

State Administrative Manual (SAM), § 4841 requires the director of each State Department that uses, receives, or provides information processing services to designate an Information Security Officer (ISO) who shall be responsible for implementing State policies and standards regarding the confidentiality and security of information within the Department. These policies and standards shall include, but are not limited to, strict controls to prevent unauthorized access of data maintained in computer files, program documentation, data processing systems, data files, and data processing equipment located physically in the Department and dissemination of information under the control of California State agencies is found in the State Constitution, in statutes, and in administrative policies:

- Article 1, Section 1, of the Constitution of the State of California defines pursuing and obtaining privacy as an inalienable right.
- The Information Practices Act of 1977 (Civil Code, § 1798, et seq.), places specific requirements on State agencies in the collection, use, maintenance, and dissemination of information relating to individuals.
- The California Public Records Act [Government Code (GC), §§ 6250-6265], provides for the inspection of public records.
- The State Records Management Act (GC, §§ 14740-14770) provides for the application of management methods to create, use, maintain, retain, preserve, and dispose of State records, including the determination of records essential to the continuation of State government in the event of a major disaster. SAM, §§ 1601-1699 contains administrative policies to implement provisions of this law.
- The California Penal Code (PC), § 502 covers the following offenses:
  - Manipulating data, a computer system, or computer network to devise or execute a fraud.
  - Knowingly accessing and, without permission, taking copies or using any data from a computer or taking any supporting documentation, internal or external, to a computer.
  - Theft of computer services.
  - Knowingly accessing and without permission, damaging data, computer software, or computer programs, internal or external, to a computer.
  - Disrupting or denying computer services to an authorized user.

The Federal Copyright Act of 1976 provides for the prosecution of persons guilty of the theft of computer programs.

49020.4 Departmental Approach to Information Security

The departmental approach to information security consists of the following components:

- Policies to ensure that information security and information privacy are incorporated at each phase of the information systems development life cycle.
- Conduct periodic risk assessments in accordance with SAM, § 4842.1, to ascertain the threats and vulnerabilities that impact the CDCR's information assets and implement appropriate mitigations.
- Provide information security training to all employees who use information assets in the course of their assigned duties to ensure awareness and understanding of the Department's policies.
- Conduct information security audits for compliance with security policies. Report deficiencies or noncompliance with the CDCR security policies to management for corrective action.
- Adherence to requirements established in SAM, § 4841.
- Periodically review security policies for changes that may be necessary as a result of technology evolution or changes in Department operations.

49020.5 Information Security Definitions

The following terms are defined for purposes of this Article:

Access

To gain entry into, or to instruct or communicate with, the logical, arithmetical, or memory function resources of a computer, computer system, or computer network.

Authorization

The granting of permission to execute a set of operations in a system.

Access Control

Tasks performed by hardware, software, and administrative controls to monitor a system's operation, ensure data integrity, perform user identification, record system access, and changes, and grant access to users.

Accountability

The ability to trace violations or attempted violations of system security to the individual(s) responsible.

Access Management Group

A group that is responsible for access permissions granted to CDCR's Information Assets, including the CDCR Network, and departmental applications and databases.

Authentication

The procedure for identifying or verifying the eligibility of a station, originator, or individual to access specific categories of information.

Baseline Security Controls

A set of general controls designed to meet an acknowledged level of security control that should be in place within all properly run computer centers.

Bulletin Board System

An electronic message system that runs a computer and allows users to enter and read information.

CDCR Network

The system of telecommunication devices, workstations, servers, and peripherals used to provide inter- and intra-facility connectivity that enable sharing of

information assets and electronic communications between CDCR employees. The CDCR Network is managed by the Office of Information Technology/Enterprise Information Systems (OIT/EIS).

Call Back

A method used to identify a terminal or modem that is dialing into a system, whereby the system disconnects the calling terminal or modem and then reestablishes the connection by dialing the telephone number of the calling terminal or modem.

Classification

The assignment of information, including a document, to a category on the basis of its sensitivity concerning disclosure, modification, or destruction.

Computer-Based Tools

Software or computer programs that improve or enable a user's ability to configure and manage information technology components.

Computer Contaminants

Any set of computer instructions that, outside the intent and without the permission of the owner of such information, is designed to modify, damage, or destroy a computer, system, or network, or to record or transmit information within a computer, system, or network. Such contaminants include, but are not limited to, the group of self-replicating or self-propagating computer instructions commonly termed viruses, trojans, and worms, which are designed to affect computer programs or data, consume computer resources, modify, destroy, record, or transmit data, or otherwise usurp the normal operation of the computer, computer system, or computer network.

Computer Network

Any system that provides communication among one or more computer systems and input/output devices including, but not limited to, display terminals and printers connected by telecommunication facilities.

Computer Program or Software

A set of instructions or statements or related data that when executed in actual or modified form, causes a computer, computer system, or computer network to perform specified functions.

Computer Security

The technological safeguards and managerial procedures that can be applied to computer hardware, programs, data, and facilities to ensure the availability, integrity, and confidentiality of computer-based resources. This can also include assurance that intended functions are performed as planned.

Computer Services

Includes, but is not limited to, computer time, data processing, or storage functions, or other uses of a computer, system, or network.

Computer System

A device or collection of device, including support devices, but excluding calculators that are not programmable and not capable of being used in conjunction with external files, one or more of which contains computer programs, electronic instructions, input data, and output data, and which performs functions including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control.

Confidential Information

Information maintained by State agencies that is exempt from disclosure under provisions of the California Public Records Act (GC §§ 6250-6265) or other applicable State or federal laws.

Critical Application

An application so important to the Department that its loss or unavailability is unacceptable. With a critical application, even short-term unavailability of the information provided by the application would have a significant negative impact on the health and safety of the public or Department employees, the fiscal or legal integrity of departmental operations, or the continuation of essential programs. All CDCR departmentwide information systems are critical applications.

Custodian of Information

An employee or organizational unit (such as a data center or information processing facility) acting as caretaker of an automated file or database.

Data

A representation of information, knowledge, facts, concepts, computer software, computer programs, or instruction. Data may be in any form, such as in storage media as stored in the memory of the computer, in transit, or as presented on a display device.

Decentralized Applications

Systems that run on more than one computer in geographically separated locations. The term also refers to systems that are not supported by a single organization, such as EIS.

Denial of Service

A situation where authorized access to information assets is prohibited because unauthorized usage has consumed all available resources. A "Denial of Service" attack is often caused by computer contaminants such as viruses and worms.

Documentation

Information about how specific applications are constructed, maintained, and used. It includes, but is not limited to, system and program design specifications, record formats, report layouts, program source and object code, job control language specifications, run instructions, key entry instructions, and data definitions.

Distributed Data Processing System

A CDCR Department information system. [Department Operations Manual (DOM), Chapter 4, Article 40, Distributed Data Processing System.]

E-mail

Written communication transmitted electronically using computers connected to network(s).

Handheld Computer

Synonym for Personal Digital Assistant.

Information Assets

Any documents, electronic files, or records that contain or are used to process, manage, or store information necessary to the operation of the CDCR.

Information Technology

All hardware and software used to collect, store, manage, and transfer information.

Information Integrity

The condition in which information or programs are preserved for their intended purpose, including the accuracy and completeness of information systems and the data maintenance within those systems.

Information Security

The protection of automated information against unauthorized access (accidental or intentional), modification, destruction, or disclosure.

Information Security Architecture (ISA)

Compilation of the strategy, guidelines, and standards comprising the CDCR's program to ensure the protection and security of information assets.

Injury

Any alteration, deletion, damages, or destruction of a system, network, computer program, or data caused by unauthorized access.

Internet

The World Wide Web (WWW), consisting of a network of networks.

Intranet

A term that refers to a closed network of networks. In the context of the CDCR, it refers to the whole of the information assets that comprise the CDCR Network.

Local Area Network

A Local Area Network (LAN) is a computer network consisting of telecommunications devices such as routers, hubs, switches, and firewalls, and computers such as workstations, servers, and peripheral devices.

Mainframe

Referring to large computers typically housed in a data center environment and running legacy systems. Mainframe computers have security components (such as Resource Access Management System) integrated into the operating system and can support many hundreds of simultaneous users.

Malicious Code

Synonym for computer contaminant.

Midrange computer

Synonym for minicomputer.

Minicomputer

A class of computers upon which applications in the 1980's were implemented that are smaller in physical dimensions than mainframes, and require less overhead to maintain. Minicomputers use terminal access and support a few hundred simultaneous users.

Owner of Information

An individual in a particular position or an organizational unit having responsibility for making classification and control decisions regarding automated files or databases.

Parole-LEADS

A departmental application used to provide parolee information to local law enforcement agencies.

PC Coordinator

An individual who supports a group of users and the information assets accessed by that group of users.

Personal Digital Assistant (PDA)

Palm-sized computer that can sync with a workstation and allow users to refer to information from the workstation without having to print it out. Schedules, e-mail, documents, and spreadsheets as well as reference material such as dictionaries and phone lists can be stored and accessed as needed. PDAs often are capable of wireless connectivity with LANs and the Internet.

Physical Security

The protection of information processing equipment against damage, destruction, theft, or unauthorized entry, and of personnel from potentially harmful situations.

Privacy

The right of individuals and organizations to control the collection, storage, and dissemination of information about themselves.

Production Application

A computer-based process that stores, manipulates, or reports departmental information.

Public Information

Any information prepared, owned, used, or retained by a State agency and not exempted specifically from disclosure requirements under the California Public Records Act, GC, §§ 6250-6265, or other applicable State or federal laws.

Resource Access Management Facility.

An application within IBM-based computer systems that reviews logons, passwords, and permissions before permitting access to information.

Risk

In the context of information systems, the likelihood or probability that a loss of information assets or breach of security will occur.

Risk Management

The process of taking actions to avoid risk or to reduce risk to acceptable levels.

Sensitive Information

Information maintained by State agencies that requires special precautions to protect it from unauthorized modification or deletion (See SAM, § 4841.3). Sensitive information may be either public or confidential.

Supporting Documentation

Includes, but is not limited to, all information in any form pertaining to the design, construction, classification, implementation, use, or modification of a computer, computer system, computer network, computer program, or computer software that is not available generally to the public and is necessary for the operation of a computer, computer site, computer network, computer program, or computer software.

Teleprocessing Equipment

Computers, network components, and other devices that facilitate, enable, or depend upon data communications. Network devices such as, but not limited to, routers, hubs, wires, computers, and servers are teleprocessing equipment.

User Identification (ID)

The logon name an individual uses to access a computer or network system.

User of Information

An individual having specific limited authority from the owner of information to view, change, add to, disseminate, or delete such information.

Victim Expenditure

Any expenditure reasonably and necessarily incurred by the owner or lessee to verify whether a system, network, data, or computer program was altered, deleted, damaged, or destroyed by the access.

Virus

A computer contaminant. Viruses are often transmitted through e-mail.

- **Wide Area Network (WAN)**

Two or more LANs connected together.

Wireless

Referring to communications transmitted without wires, such as radio, microwave, or infrared.

Workstation

Any device commonly called a microcomputer, PC, or terminal used for processing, storing, or sending information.

Worm

A computer contaminant. Worms are often introduced into a LAN or WAN through e-mail and then propagate themselves to other workstations on the network.

- **WWW**

An abbreviation for World Wide Web. See Internet**.**

49020.6 Responsibility

The Department has established the necessary policies, procedures, practices, and controls to protect information assets from accidental or intentional disclosure, destruction, or modification, and to comply with all applicable State and federal privacy legislation. Information assets covered by this Article include, but are not limited to:

- All categories of automated information including, but not limited to, records, files, and data bases.
- Information technology facilities, software, and equipment (including personal computer systems) owned or leased by the CDCR.

The following is a description of the organizational responsibilities for administering this program:

Secretary

The Secretary is responsible for establishing and maintaining an information security program within the Department. It is the responsibility of the Secretary to assure that information assets are protected from the effects of damage and destruction, as well as from unauthorized or accidental modification, access, or disclosure. Specifically, the Secretary is responsible for ensuring:

- Enforcement of State level security policies.
- Establishment and maintenance of internal policies and procedures that provide for the security of information technology facilities, software and equipment, and the integrity and security of the agency's automated information.
- Department compliance with reporting requirements related to security issues.
- Appointment of a qualified Information Security Officer (ISO).
- Participation of management during the planning, development, modification, and implementation of security policies and procedures.

ISO

SAM, § 4841 requires that each agency designate an ISO. Additionally, to avoid conflicts of interest, the following restrictions shall apply to the ISO:

- The ISO shall not have direct responsibility for information processing.
- The ISO shall not have direct responsibility for access management functions.
- The ISO shall not have direct responsibility for any departmental computer-based systems, or have a reporting relationship to an organization thathas such responsibility.
- The ISO shall not have any special allegiance or bias toward a particular program or organization.

The ISO is responsible for overseeing Department policies and procedures designed to protect its information assets. In accordance with State policy, the ISO shall be accountable to the Secretary with respect to these responsibilities.

The responsibilities of an ISO include overseeing the following:

- Implementation of necessary procedures to ensure the establishment and maintenance of a security program.
- Establishment of security policies and procedures designed to protect information assets.

- Identification of confidential and sensitive information and critical applications.
- Identification of vulnerabilities that may cause inappropriate or accidental access, destruction or disclosure of information, and establishment of security controls necessary to eliminate or minimize their potential effects.
- Establishment of procedures necessary to monitor and ensure the compliance of established security and risk management policies and procedures.
- Coordination with internal auditors to define their role in automated information system planning, development, implementation, operations, and modifications relative to security.
- Coordination with the applicable data center's ISO or staff on matters related to the planning, development, implementation, or modification of information security policies and procedures that affect the Department.
- Acquisition of appropriate security equipment and software.
- Establishment of procedures to comply with control agency reporting requirements.
- Development and maintenance of controls and safeguards to control user access to information.
- Establishment of mechanisms to assure that Department staff (with particular emphasis on the owners, users, and custodians of information) are educated and aware of their roles and responsibilities relative to information security.
- Establishment of training programs for Department employees related to information security.

Technical Management

Department technical management has the following responsibilities relative to the Department's information security program:

- Ensuring that management, the ISO, assigned owners, custodians, and users are provided the necessary technical support services with which to define and select cost effective security controls, policies, and procedures.
- Ensuring the implementation of security controls and procedures as defined by the owners of information.
- Ensuring the implementation of system controls necessary to identify actual or attempted violations of security policies or procedures.
- Ensuring that the owners of information and the ISO are notified of any actual or attempted violations of security policies and procedures.

Program Management

Department program managers have the following responsibilities in relation to the Department's security program:

- Establishing the procedures necessary to comply with State information security policy in relation to ownership, user, and if appropriate, custodian responsibilities.
- Ensuring that State program policies and requirements are identified relative to security requirements.
- Ensuring the proper classification of automated information for which the program is assigned ownership responsibility.
- Ensuring the participation of the ISO and technical staff in identifying and selecting appropriate and cost-effective security controls and procedures, and to protect information assets.
- Ensuring that appropriate security requirements for user access to automated information are defined for files or data bases for which the program is assigned ownership responsibility.
- Ensuring the proper planning, development, and establishment of security policies and procedures for files or data bases for which the program has ownership responsibility, and for physical devices assigned to and located in the program area(s). Ensuring that custodians of program information are provided the appropriate direction to implement the security controls and procedures that have been defined.
- Ensuring that procedures are established to comply with control agency reporting requirements.

Program Personnel and Users

Program personnel have the following security responsibilities:

- Implementing and monitoring data quality assurance functions to ensure the integrity of data for which the program is assigned ownership responsibility.
- Complying with applicable federal, State, and Department security policies and procedures.
- Complying with applicable federal and State statutes.
- Identifying security vulnerabilities and informing program management and the ISO of those vulnerabilities.
- Ensuring that management, the ISO, and assigned owners, custodians,and other users are provided the necessary technical support services with which to define and select cost-effective security controls, policies, and procedures.
- Ensuring the implementation of security controls and procedures as defined by the owners of information.
- Ensuring the implementation of system controls necessary to identify actual or attempted violations of security policies or procedures.
- Ensuring that the owners of information and the ISO are notified of any actual or attempted violations of security policies and procedures.

Internal Auditors

The Information Security Unit of the Office of Audits and Compliance has the following audit responsibilities in relation to the Department's information security program (DOM, Chapter 4, Article 48, Electronic Data Processing Auditing).

- Examination of the Department's information security policies and procedures for compliance with State information security policies, including control agency audit requirements.
- Identification of possible corrective actions.
- Informing management, the ISO, and the owners, custodians, and users of information of audit findings.

Access Management

Access Management within the CDCR is:

- A critical responsibility of information system owners and custodians.
- An organizational unit within the EIS.

The access management group and each organization with owner or custodial responsibilities for an information system have the following access management responsibilities:

- Access Authorization. The granting of permission to execute a set of operations in the system. At the lowest level, for example, this would be to grant permission for inmate trust personnel to access the classification of inmates on the Distributed Data Processing System (DDPS). At the highest level, for example, this would be working with the information system owners to physically allow access to a specific information system.
- Access Control. Enabling the performance of tasks by hardware, software, and administrative controls that would have the effect of monitoring a system's operation, ensuring data integrity, performing user identification, recording system access and charges, and granting access to users.
- Accountability. The work necessary to set up the ability to trace violations or attempted violations of system security to the individual(s) responsible.
- Additionally, the access management group of the EIS shall maintain the central file of all signed self/joint certification statements and security agreements, and shall provide the ISO, management, and owners with appropriate status reports.

Information Security Coordinators

Every organizational entity that uses computer systems, or uses computer applications that are not directly supported by the EIS shall designate an Information Security Coordinator (ISC) for each site maintained by that entity. The designated Security Coordinator shall be responsible for ensuring that applicable CDCR policies and procedures are followed, and shall act as the security liaison to the ISO.

A procedure shall be developed by each of these organizational entities, subject to approval by the ISO. The procedure shall be constrained as follows:

- The designation of an ISC for the decentralized or control entity shall be in writing and shall identify the name, work address, and telephone numberof the ISC.
- The access management group shall maintain a file of all current and past designated ISCs.
- The designated ISC shall be aware that they are the designated Security Coordinator and the responsibility that the designation entails.

- The designated ISC shall ensure compliance with information security policies and procedures, and with any security guidelines issued by the owners of decentralized automated systems.

Information Owners

The owners of information are responsible for classifying the information, defining precautions for its integrity, disposing of the information, defining initial levels of access need, filing security incident reports, securing signed security agreements, and forwarding them to the Access Management Group, and identifying for the ISO the level of acceptable risk.

Each information system has one or more owners that are identified as part of the approval process for system development. Information owners must approve all major changes to information systems.

Information Custodians

The custodians of information, including the Teale Data Center, are responsible for complying with applicable laws and policies and procedures established by the owner and the ISO, advising the owner and the ISO of any threats to the information, and notifying the owners and the ISO of any violations of security policies, practices, and procedures.

49020.7 Reportable Incident Criteria

It is the responsibility of all departmental employees to report all incidents that would place the Department's information assets at risk. The following incidents shall be reported through the local ISC and chain of command to the Chief Deputy Secretary and to the departmental ISO within three days of becoming aware that an incident has occurred:

- Unauthorized access to, or modification of, State-owned or State-managed data, including nonelectronic data such as reports, documentation, and hard copy files.
- Unauthorized use of, or access to, State computer resources, including computer networks and services as well as systems not necessarily connected to a network.
- Unauthorized access to, or modification of, computer software, including operating systems, networks, configurations, and applications. This includes the introduction of malicious software such as viruses, worms, and other malicious software.
- Deliberate or unauthorized acts resulting in disruption of State computer services, including "Denial of Service" attacks.
- Unauthorized use of user account or Internet domain names.
- Destruction of, or damage to, State information processing facilities.
- Break-in or other unauthorized access to State facilities resulting in compromise to the data or computer systems housed within those fcilities.

CDCR management shall investigate all incidents.

49020.7.1 Incident Report Format

The following information concerning each incident shall be reported to the ISO within three working days of becoming aware of the occurrence of the incident:

- Date and time.
- Location.
- Description of what happened.
- Estimated damages.
- Description of corrective action, taken or planned.
- Estimated costs associated with corrective actions.
- If known, identity those responsible for the incident.
- Descriptions of actions taken or planned against those responsible for the incident.
- Contact name and phone number.

The report submitted to the ISO shall be signed by the appropriate Warden, Regional Parole Administrator, Director, or Assistant Secretaries. Incident reports shall be forwarded to the Department of Finance (DOF) within five business days of the initial report, and shall be signed by the ISO. The Highway Patrol shall be notified of the occurrence of an incident within one day of receipt of the initial report.

49020.7.2 Consequences of Information Security Violations

During the time that a suspected violation is under investigation, the suspected violator's access privileges may be revoked or other appropriate action taken to prevent harm to the CDCR.

All violations of security policies or procedures are subject to disciplinary action. The specific disciplinary action that shall be taken depends upon the nature of the violation and the impact of the violation on the CDCR's information assets and related facilities. A partial list of potential disciplinary actions follows:

- Written reprimand.
- Suspension without pay.
- Reduction in pay.
- Demotion.
- Dismissal.
- Criminal prosecution (misdemeanor or felony, State or federal).

49020.7.3 Failure to Correct Information Security Deficiencies

Should any audit indicate that the State's security policies are not established or that the Department has not taken corrective action with respect to security deficiencies, the Department may be subject to any or all of the following:

- Further audit and review by the Financial Performance Accountability Unit of the DOF.
- Revocation by the DOF of delegated approval authority for information technology projects.
- Application of penalties specified in GC, § 1222.

49020.8 Information Security Ownership/Authority

An owner of CDCR information must approve all requests for access to such information under his or her control. Approval authority may be delegated to a designated representative. The owner has an obligation to restrict access to the specific information to instances that are necessary and sufficient to meet the demonstrated need or right of the requestor. The owner shall consult with EIS to determine the most appropriate on-line access mechanisms for a specific request, keeping in mind that EIS is obligated to restrict the mechanisms to those that are necessary and sufficient to meet the requestor's need for, or right to, such information.

The owner is ultimately responsible for the integrity of the entrusted information. This responsibility requires that the owner have control over who can access, modify, disclose, or destroy information. The owner shall exercise the responsibility to communicate information security requirements to all appropriate personnel, and to make use of all available security features. Additionally, the owner shall determine that implemented security measures are adequate to meet the requirements of the application, and ensure that an employee's access authority is removed immediately upon separation or change of duties such that access is no longer necessary.

49020.9 Confidentiality of CDCR Information Assets

For administrative purposes, all information residing on CDCR's computers that is considered to be sensitive or confidential shall be treated as such by all persons who have access to it and shall be protected from unauthorized access.

No confidential information shall be present on any computer resource, including workstations, that is not under CDCR's direct control unless authorized on a case-by-case basis by the ISO and the owner of the information.

Appropriate procedures to utilize confidential CDCR information on any of CDCR's computer resources, including any computer such as mainframes, mid-range, workstation, and other information assets on the CDCR network are outlined in this Article. The level of security measures shall be commensurate with the classification of the information involved.

49020.9.1 Confidentiality of Security Mechanisms

The specific security mechanisms used by the Department to control access to its information resources are confidential.

Information concerning specific details of access controls shall not be divulged except on a need-to-know basis, and only then to persons for whom there are signed security agreements on file.

49020.9.2 Confidentiality of Production Application Software

All documentation concerning production applications residing on CDCR's mainframes, midrange, and workstations is confidential.

Appropriate procedures to protect and preserve the confidentiality of applications documentation are to be developed by each division that has responsibility for, or custody of, such documentation. The procedures shall ensure that documentation is not divulged except on a need-to-know basis, and only then to persons for whom there are signed security agreements on file.

49020.9.3 Confidentiality of Information on CDCR Information Systems

Appropriate procedures shall be developed by each CDCR Division to protect and preserve the confidentiality of the Department's information stored or residing in or on CDCR controlled environments, such as the CDCR Network, individual stand-alone desktop and laptop workstations, browser-based applications such as Parole-LEADS, and the DDPS. Additionally, no confidential information shall be faxed, reproduced (e.g., photocopied), distributed via e-mail, downloaded to a nonconfidential system, given to an unauthorized recipient, or transmitted by telephone to any entity without appropriate security controls in place that are documented in the CDCR ISA.

49020.10 Access to Information Assets

Access to any CDCR computerized information on any CDCR computers or the Teale Data Center is restricted to authorize persons. Any person requiring such access shall:

- Be a State employee or a bona fide representative of the Department.
- Demonstrate either a need for, or a legal right to, the information.
- Receive formal authorization from the owner of the information.
- Accept legal responsibility for preserving the security of the information.

The sensitivity of the information residing in CDCR's computerized environments requires strict controls over who is allowed access to that environment, which information may be accessed, and how that information may be accessed.

The following uniform access authorization procedure assumes that all pertinent procedures have been followed, and all CDCR-required system approvals have been obtained. This procedure is for access to existing information resources.

The uniform access authorization procedure is as follows:

- The requestor shall complete a risk analysis. The risk analysis shall address all threats created by the additional access requirements and the necessary controls.
- All access requests, including the risk analysis, shall be sent to the system owner with a copy to the ISO. The request shall contain the following:
  - The name of the requester.
  - The specific information for which access is desired.
  - The reason(s) why the requestor has a need for, or right to, the information.
  - The frequency and duration of the requested access.
  - The type of access (e.g., read, update, copy, etc.).
  - An approval signature block for the owner's approval.

After the owner approves the request for access and returns it to the requestor, the approval is then routed to either EIS or the requesting organization's ISC for action.

49020.10.1 Annual Information Security Self-Certification

All CDCR employees requiring access to CDCR information assets are responsible for annually self-certifying that they are in compliance with applicable CDCR information security policies. The ISO is responsible for ensuring compliance with this policy. Responsibility for the dissemination of the policies rests with the owner and the designated security coordinator; responsibility for compliance rests with the end-users.

Appropriate decentralized and control entity procedures shall be developed by each CDCR unit that owns or has custody of decentralized applications including, but not limited to, the applications delineated in DOM, Chapter 4, Article 31, Personal Computer Systems, CDCR Network access, use of stand-alone computers to complete CDCR work, and access to the Internet. Each such procedure is subject to approval and audit by the ISO. The procedures are constrained by the following:

- A separate statement of self-certification shall be signed by every employee that access or uses CDCR's information assetts.
- Each self-certification shall be signed by a representative of the senior management of the organizational entity.
- Each self-certification is to be filed with the local ISC and available for review by the ISO.

49020.10.2 Information Security-Responsibilities of Password Owners

Access to CDCR's information systems is restricted by password to only authorized persons. Authorized persons shall never reveal their passwords to anyone for any reason. Authorized persons using a computer shall log off or activate a password-protected screensaver before leaving the immediate vicinity of the computer or terminal. Additionally, no ability shall exist for a user to store, load, or invoke the log on process on any CDCR computer, by any method that includes the user Resource Access Control Facility (RACF), ID, or the password. Violation of this Policy may result in the revocation of all access privileges and appropriate disciplinary action. Such disciplinary action may be based not only on the violation itself, but also on all activity performed by those obtaining access to a system or information asset due to a violation of this Policy.

The password is a major "key" to the integrity of CDCR's automated environment. The password policy exists to protect the integrity of that "key."

User IDs shall never be shared. User ID security is backed up by the existence of passwords. Owners are responsible for anything for which their password is used. Therefore, as a matter of self-protection, the password owner shall:

- Not tell anyone what the password is.
- Not write down the password.
- Not use an obvious password. Obvious passwords include one's name or nickname, the names of one's children, one's user ID, names, or words associated with hobbies ("DANCER," "SKIER," "GOLFER," etc.), names associated with favorite books, TV shows, or movies ("JEDI," "FRODO," "PICARD", "RHETT," etc.), "SECRET," "SECURE," "PASSWORD," all spaces or the "enter" key, "9999999", "XXXXXXX," driver's license, social security numbers, the name of the current month, etc.
- Not use words that can be looked up in any dictionary, including foreign languages (e.g., Latin).
- Use non-obvious passwords, such as word combinations rather than single words ("COMPUTERUSER," "SKIBUM," "IAMADANCER," etc.) intentionally misspelled words ("KRAKER," "KORECTUNS," etc.), or random combinations of letters and numbers, etc.
- Use passwords that are at least seven characters long.
- Change the password in accordance with specific application requirements, every 30 to 90 days, depending on the application.

If the password owner becomes aware that a correct password is being rejected, that user should immediately notify the local ISC and the ISO, since this may indicate that someone has discovered the password and has changed it without the owner's permission, resulting in the owner no longer knowing his or her own password.

If a password is forgotten, the local ISC or the CDCR Help Desk shall be contacted. They shall validate the owner's identity and give a new temporary, one-time password. The owner shall change this password immediately.

If anyone asks for a password, the owner shall refuse to provide it and shall refer the person to a supervisor. The owner shall then notify the supervisor.

Anyone who knows that any password has been compromised should take the following actions:

- Notify the ISC.
- Notify the ISO.
- Complete a "security incident report."

49020.10.3 Information Security-Responsibility of Supervisors

People are provided passwords because their jobs require them to access CDCR information systems. When a password owner terminates employment or is reassigned to duties that do not require such access, the immediate supervisor shall, without delay, notify the applicable party of the change.

The authority to access CDCR computers entails a significant risk to the Department's ability to function. Such authority is restricted to persons with a demonstrated need for access. Because that need is, by definition, a function of the person's specific job duties, any change in those duties requires a reevaluation of the need for access. If the duties change such that the need for access no longer exists, the access shall be revoked.

If any password owner changes job duties (via resignation, promotion, transfer, reorganization, separation, etc.), that individual's immediate supervisor shall initiate the following:

- Reevaluate whether the person's new duties still require the authority to access CDCR's computers.
- Notify the local security coordinator or the access management group if the person no longer requires access authority.

- Notify the owner of the relevant CDCR information so that the appropriate paperwork can be initiated to document the removal of the person's access privileges if the person no longer requires access authority.

The lack of use of the access authority is assumed to be proof that the authority is no longer required. Access authority to information assets may be revoked without notice if they are not used regularly.

49020.10.4 Requesting Authority to Access CDCR's Mainframe Environments

Access to an entire mainframe environment shall not be authorized. Access to specific portions of that environment, such as, but not limited to, the system development facilities, shall be authorized for specific organizations. Access to a specific application can be authorized by the Information Owner as a means of meeting a specific request for specific information.

49020.10.5 Unattended Workstations

Active workstations or terminal sessions must not be left unattended. Any authorized or unauthorized activity on an unattended workstation will be attributed to the person whose logon and password activated the terminal or workstation. All sessions shall either be terminated when leaving the immediate area, or protected with a password-activated screensaver.

49020.11 Restrictions on Using CDCR Information Assets

The use of all CDCR information assets including any mainframe computers, minicomputers, notebook, laptop and workstation desktop systems, network components, and applications run on or accessed from CDCR computers is restricted to official CDCR business.

49020.12 Information Systems Access Control

All access to CDCR's information systems shall be protected by at least user ID/password access control. CDCR's mainframe computers shall operate within the constraints of RACF. Any software installed on mainframe computers that uses its owner password protection features shall provide for nondisplay of, and restricted control over, passwords.

Because RACF is the facility used to logically protect the resources on the CDCR's mainframe computers, no software that allows RACF to be bypassed or compromised may be installed on those computers.

49020.13 Segregation of Duties in the Information Security Program

There shall be a strict separation of duties between, and within, all organizations responsible for using, operating, and developing computer-based information systems. Separation of duties shall be maintained to ensure a separation of responsibilities for initiating and authorizing transactions, recording of transactions, and custody of assets. Segregation of duties, similar to that required in manual systems, shall be implemented in computerized systems.

The following guidelines shall be used regarding such separation of duties:

- Convert and conceal - No one person should be able to convert a resource to their personal use and be able to conceal the action.
- Custody and control - No one person should have custody of an asset and at the same time be solely responsible for the accounting for that asset.
- Custody and access - No one person shall have custody of an asset and, at the same time, have unrestricted access to the records pertaining to that asset.
- Origination and authorization - No one person shall both originate and authorize a transaction.
- Originate and maintain - No one person shall both enter a transaction and maintain the related master file.
- Access and restriction - Access to transactions shall be on a need-to-know basis.

EIS is charged with the responsibility for the development and maintenance of computer-based systems for the CDCR. In this capacity, EIS provides a service to actual or potential users of computer-based information systems. In addition, there are several computer "users" groups throughout the Department. Each of these organizations is providing a service to all actual or potential users of computer-based information systems.

To ensure that assigned responsibilities are met and that separation of duties is maintained, individuals/programs shall not originate or authorize transactions, have custody or control over online data processing assets, or have the authority to originate master file changes. Source documents shall originate and be controlled by functions independent of such persons/programs.

Appropriate procedures shall be developed by the EIS, subject to approval by the ISO, to ensure that adequate controls exist to ensure the separation of duties and responsibilities.

The procedures may include variances to the Change Management Process in order to resolve failures of critical applications. Such variances shall provide for audit trails and retroactive release or approval documentation, and require the prior approval of the ISO.

49020.14 Information Security Awareness

It is the responsibility of CDCR management at all levels to ensure that personnel are aware of their responsibilities:

- All employees are accountable for the implementation of information security policies and procedures within their areas of responsibility.
- Accountability requires that employees be aware of the Department's information security policies and procedures.
- All employees that are owners, users, or custodians of a departmental information system shall receive annual information security training.
- Security awareness training shall be given as a part of each employee's orientation and annually thereafter. Each employee shall receive a copy of the security policy. All employees that access or use information assets shall annually complete and sign a self-certification form.
- All employees changing jobs or exiting owner, user, or custodian status, shall have their security privileges revoked immediately, and such persons shall be prevented from having any further opportunity to access information.
- Employees with the status of owner, user, or custodian shall have a job descriptions that details that status and the security requirements therein.
- Systems, including CDCR's mission critical systems and Internet access, shall be monitored and activity logs maintained as per the Department's ISA.

49020.14.1 Security Awareness Training within CDCR

All persons who have access to any CDCR information shall be provided security awareness training at the time such access begins, and at least annually thereafter. The ISO shall ensure that security awareness training is provided prior to the employees' self-certification of their awareness of CDCR's information security policies, and the renewal of access privileges to CDCR information assets.

Security awareness training falls into the following two categories:

Information Security

All individuals having access to CDCR information shall be made aware of the background, scope, and objectives of CDCR's information security program and of specific CDCR information security policies and procedures that are applicable to the level and type of access granted to the individual. The minimum training shall consist of completion of the departmental computer-based training module.

Incident Reporting

All CDCR employees shall also be made aware of the events and activities that constitute threats to the organization for which they work and of the actions to be taken when confronted by those events or activities.

49020.15 Physical Access Control to Information Assets

The sensitivity of CDCR's information assets and personnel safety requires that all CDCR computer facilities have physical controls to prevent unauthorized access.

Each owner and custodian of departmental information systems shall establish physical controls over their information assets. This requirement applies to workstations with confidential or sensitive information and includes network and data communications components, as well as, application and database servers.

49020.16 Confidential or Sensitive Information Stored on Workstations

The nature of information classified as confidential or sensitive requires strict controls over access to such assets (SAM, § 4989.7).

Confidential or sensitive information may be stored on or accessed with workstations in accordance with the following provisions.

- Only authorized personnel may have access to confidential or sensitive data.
- Workstations containing or capable of accessing such data shall be equipped with hardware and/or software that provide for authentication techniques, such as password protection of confidential files.
- Confidential and sensitive files shall be encrypted, if the owner deems it necessary. Encryption software must comply with standards documented in the ISA.
- Backup files of confidential data shall be maintained in a locked cabinet away from the location of the workstation containing the program providing access to such files.

- Security hardware/software shall comply with standards documented in the ISA.
- At least two individuals shall be authorized access and have knowledge of the location where data files, backup files, and forms are stored.

49020.16.1 Software Controls on CDCR's Workstations

The following software controls shall be established for all CDCR workstations:

- No software shall be loaded, installed, and/or activated on any CDCR workstation without prior review and written approval from the local ISC and the requestor's supervisor, or EIS.
- Controls that ensure that the CDCR is in compliance with all State-mandated requirements (SAM, §§ 4820, 4989.7, and 4990.1).
- Appropriate procedures shall be developed by ISCs for use by each CDCR division that has workstations. These procedures are subject to approval by the Department's ISO, and are constrained by the requirements of the CDCR workstation policy.

49020.16.2 Data File Transfers

Electronic transfer (file transfer) of information to or from any CDCR information system file or database is restricted to authorized persons who shall use an approved file transfer mechanism. The same level of protection afforded the information in its originating system shall be provided by the computer environment to which the information is transferred.

Transfer of information from one CDCR computer to another does not alter the sensitive nature of the information or eliminate the need to protect the confidentiality of the information. An appropriate procedure shall be developed by EIS for use by each CDCR division that uses file transfer mechanisms. The procedure shall be constrained as follows:

- The user is responsible for providing the necessary controls to secure all confidential information maintained in the workstation environment. A Security Plan must be approved by the ISO prior to confidential or sensitive information being stored on a workstation.
- Dial-up access to the Department's databases is prohibited.
- All requests to transfer information shall be approved by the owners of the information and the custodians of the information. The owners shall provide the necessary authorization for access (if the request is approved) and the custodian shall provide the methodology.
- Confidentiality of information shall be maintained.
- Any workstation performing file transfers shall be subject to additional hardware and software controls (e.g., encryption and dynamic password user authentication) to enhance the security environment of the workstation.

Interagency data file transfers are subject to requirements described above as well as those defined in DOM, Chapter 4, Article 45, Information Security, § 49020.5.

49020.17 Information Security Architecture

Teleprocessing equipment in CDCR's automated network environment (computers and peripherals) shall be secured against access by unauthorized persons. Any equipment that is not stand-alone is considered teleprocessing equipment. This includes all workstations that are connected to each other or to any other mainframe, mini or micro, whether by dial-up, cabling (including, but not limited to coax, twisted pair, and fiber), LANs, Gateways, routers, and all other network components. Access to CDCR's network shall be restricted to CDCR employees. The methods by which CDCR's teleprocessing equipment is secured shall be documented in the CDCR ISA. Any exception or modification to the ISA must be approved in writing by the ISO prior to implementation.

The ISA shall include descriptions of procedures to protect and preserve the teleprocessing equipment from access by unauthorized persons. The procedures are constrained by the following:

- Only authorized personnel shall have access to terminals, printers, control units, concentrators, telephone wiring panels, modems, and emulation cards.
- Control of access through the CDCR telecommunications system to the Internet is the responsibility of the EIS, and is administered in accordance with the ISA. Additional access not described in the ISA constitutes a request for a modification to the ISA and must be submitted and approved in accordance with this policy prior to implementation.
- Persons not authorized to access the CDCR's telecommunications system shall obtain approval from the designated local ISC. Unauthorized persons include representatives of control agencies, CDCR personnel from another site, equipment vendors, telephone companies, etc.
- Any division with custodianship of decentralized applications shall locate equipment in restricted areas that shall be monitored during working hours and locked during unattended periods.
- Access to computers, either connected to a CDCR network or stand-alone, shall be limited by the use of a password-protected screensaver and/or key-controlled access to the power supply and/or keyboard with the keys physically removed and stored away from the workstation.
- Computers connected in any way to CDCR's telecommunications system or stand-alone computers with modems connected to them may not be located in areas where inmates have access, except when work assignments involve janitorial duties and the inmates are under the direct and constant supervision of custody staff.
- Control units shall be locked whenever possible and the keys removed and stored in a secure environment.
- Storage media including, but not limited to diskettes, CDs, removable hard drives, and tapes shall be removed from equipment that reads them and stored in a secure environment when not in use.
- Documentation pertaining to the hardware, system software, and configuration of the CDCR's telecommunication system are confidential.
- All facility phone rooms and other locations where network components are kept shall be labeled "Out of Bounds. Authorized Personnel Only."

49020.17.1 Requests for Modifications of the Information Security Architecture

The sensitivity of the CDCR's automated information assets requires strict controls over who can use equipment that is configured to access these assets. Also, the monetary value of the equipment itself warrants physical controls to deter theft or damage to the equipment.

A risk analysis shall be carried out prior to any major change to the Department's data networking capabilities. This risk analysis must be conducted in accordance with DOM, Chapter 4, Article 46, Information Systems Risk Management, and submitted with a description of the proposed change and reasons for considering the change, for approval to the ISO prior to implementation of the proposed changes.

Changes in the physical location of telecommunications equipment and switching of terminals and computers from one control unit to another require approval of the network owner (in most cases the EIS).

The teleprocessing coordinator's staff shall conduct the actual activities.

49020.17.2 Modem Usage

The critical and sensitive nature of the informational resources residing in CDCR's computers requires stringent controls of devices attached to these computers, and over which persons are allowed to use these devices.

All access to the CDCR's systems shall be monitored and controlled by EIS. All other means of accessing CDCR systems including, but not limited to, wireless communication devices and dialup modem, are prohibited unless approved by the ISO.

Modem use is restricted to computers not connected to the CDCR Network, unless such use is an approved part of the ISA. Requests for additional modems to be used within the CDCR teleprocessing environment are subject to approval.

Modems may be used to access remotely the CDCR network resources through EIS-supported access mechanisms. They may also be used to provide access to the Internet and specific destinations and e-mail capability when such access is not available through the CDCR network resources. Justification and procurement of modems for these purposes shall be conducted in accordance with DOM, Chapter 4, Article 41, Departmental Workgroup Computing Policy.

Specific restrictions on the use of modems are:

- There shall be no inmate or parolee access to any computer for which a modem has been approved. Computers that are attached to modems shall not be located in areas where inmates or parolees have access.
- No applications that were developed by inmates shall be implemented on a modem-equipped computer.
- No modems shall be installed on any computer that is a part of a LAN that has been approved for inmate use.

- The location and usage of all modems must be tracked and monitored at all times.
- Computers with "pocket" modems may not be used within the secured perimeter of facilities. They shall not be used in parole offices unless the area where the modem is to be used is secured from parolee access.
- Non-CDCR computers shall not access the CDCR Network via modem.

49020.17.3 Documentation of Changes to CDCR's Teleprocessing Environment

Any modification to the ISA must be accompanied by a risk analysis and must be approved by the ISO.

An appropriate telecommunications change log and logging procedure shall be used by the EIS to provide an audit trail of all approved changes to the ISA. At a minimum, this log shall contain entries for the following:

- Alterations in the number, type, or location of terminals, control units, modems, concentrators, phone lines, ports, protocol converters, front-end processors or communications controllers, encryption-decryption devices, dial-up ports, etc.
- Changes to the existing control software configuration, such as new additions, releases, modification, and version changes.
- Changes due to new applications.

Changes to on-line applications if those changes impact the vulnerability or integrity of the Department's teleprocessing environment.

49020.17.4 Installation of Changes to CDCR's Teleprocessing Environment

Changes to the teleprocessing environment that require a modification to the ISA shall not be implemented without the documented approval of the ISO.

This Section is intended to ensure the maintenance of adequate controls over the teleprocessing environment. The ISA policy provides a method for identifying the teleprocessing environment changes that have a security impact.

CDCR's access management group is responsible for installing certain types of the teleprocessing environment changes into production. The ISO shall provide the access management group a copy of the notification form for each teleprocessing environmental change that:

- The access management group is responsible for installing into production.
- Is identified as having a security impact.

49020.17.5 Accessibility of Mainframe Systems

Access to mainframe systems software is restricted to the EIS. Access to mainframe systems software for any other organization or individual is forbidden. Exceptions shall be granted only after a thorough review within EIS, and approval of the ISO. If it is essential that mainframe systems software access be provided, it shall be restricted to the specific commands, such as Clists, Procs, Panels, and Applications that are necessary and sufficient to meet the informational needs of the specific organization or individual, and such access shall be restricted to the time frame appropriate to the user's needs.

The power of the tools available in mainframe systems constitutes such a risk to the security and integrity of CDCR's sensitive information resources that their use shall be severely restricted.

All requests for temporary or short-term user IDs (e.g., user IDs for contract programmers) shall indicate that they are limited term requests and shall specify the estimated date on which the user ID shall no longer be needed.

Requests for access to environments other than that normally given shall include justification.

49020.17.6 Physical Security Controls

No unauthorized hardware (e.g., line monitors, modems, nodes, gateways, bridges, etc.) or unauthorized software (refer to approved list maintained by the EIS) shall be loaded, installed, or activated on any system connected to the CDCR Network. Any installation that requires a modification to the ISA must be approved by the ISO prior to implementation.

The installation of non-CDCR teleprocessing equipment, including computers, network, and communications devices is prohibited without prior written approval from the ISO.

Implementation of non-CDCR teleprocessing equipment must adhere to the same security policies governing the CDCR teleprocessing equipment, specifically those policies regarding inmate access to computers and areas where computers are used.

Portable and handheld telecommunications devices such as pagers, cell phones, and palm-sized computers are not allowed in inmate-accessible areas without prior written approval of the ISO.

The purpose of this Section is to provide controls to ensure that the CDCR is in compliance with all mandated guidelines (SAM, § 4989.7) and to protect accessible information residing on a LAN system.

49020.18 Inmate Use of Computers

It is the policy of the Department to allow inmates or parolees access to computers, computer terminals, or computer keyboards only within the constraints of the policies contained in this Article.

Any request for exception shall be referred to the ISO for review.

49020.18.1 Restrictions on Computer-Knowledgeable Inmates

Inmates who have a history of computer fraud or abuse, as defined in Penal Code (PC), § 502, shall not be placed in any assignment that provides access to a computer.

Inmates that have documented histories of computer fraud or abuse, as noted during the initial classification process, shall be identified on the initial classification chrono. Any occurrence of computer abuse after admittance to the prison system shall also be recorded in the inmate's records.

Inmates who have knowledge of computer use, programming experience, or other skills that exceed assigned staffs' ability to monitor their activity on computers, may not access computers. Staff assigned to supervise inmates using computers shall be able to monitor inmates' activity.

49020.18.2 Inmate Access to Computer-Based Tools

Inmates shall not be allowed access to any computer-based tools that could be utilized to create a virus, trojan, worm, or cause damage to data files or a computer's operating system, except in an approved Computer Refurbishment Program.

49020.18.3 Inmate Access to Computers and Telecommunications Devices

Inmates may access workstations for the purpose of completing specific tasks or assignments while under direct and constant supervision. The approved uses of workstations by inmates shall be carried out only under very tightly controlled circumstances:

- Each computer shall be labeled to indicate whether inmate access is authorized.
- Computers used by inmates shall not be used concurrently for any other purpose.
- The local ISC shall approve or disapprove the movement of computers from an "inmate use" status to other work and vice versa.
- Inmates with a work assignment involving a particular computer shall not be assigned to work on other computers.
- Areas where inmates are authorized to work on computers shall be posted as such.
- All inmates shall be under the supervision of a knowledgeable employee within a controlled, designated area when using computers.
- There shall be no communications capabilities in the designated area, such as a telephone line, computer network line, telephone punch panel, cell phones, wireless communication devices such as pagers or handheld computers or radio communication devices.
- Inmates shall not have access to computer utility programs used to modify the functionality of the computer or to view system configuration information, except in an approved Computer Refurbishment Program.
- Inmates shall not have electronic storage media in their possession except within an approved area.
- Inmates may not have access to computer application development tools.
- An inventory and appropriate controls shall be maintained on all diskettes. Diskettes for inmate use shall be labeled "For Inmate Use." Reports and other printed output from inmate-utilized computers shall be reviewed closely by staff, and appropriate distribution of such output shall be monitored.

- Inmates shall not have access to the operating system of any computer. Inmates shall not have access to any interface that allows access to the system configuration of any computer including, but not limited to, dialogue boxes, setup, and configuration screens. Additionally, inmates shall not have access to operating system commands that allow viewing or modification of any aspect of a computer operating system or the configuration of a computer, except in an approved Computer Refurbishment Program.
- Inmates shall not be allowed to load software onto hard disks, except in an approved Computer Refurbishment Program.
- No inmate shall have access to, or possesion of, any telecommunication capability, including Internet accessible computers, wireless devices such as pagers or handheld computing devices or cell phones.
- There shall be no inmate access to a computer outside the inmate's authorized work, vocational, or educational areas, unless approved by the ISO.

49020.18.4 Operation of Computer Programs Created by Inmates

Any computer-based system that was created by inmate programmers that is used to accomplish or complete the CDCR-related work shall not be operated or maintained by any inmate.

49020.18.5 Supervision of Inmates Using Computers

The persons responsible for supervising inmates' use of computers shall certify in writing that these policies are being adhered to at their specific site.

A copy of this certification shall be kept on site by the local ISC.

49020.18.6 Education Computers

The use of computers for academic and vocational education is subject to the same requirement of due care applying to all personnel that use computers within applicability of the Department's information security and risk management program.

49020.18.7 PIA Systems

Inmate use of computers in PIA and in CDCR facilities shall be in accordance with the departmental policies and institutional procedures.

49020.19 Information Security-Warnings

All critical Department systems shall display a warning at the first screen that any user of the system will see when the computer system is accessed.

49020.20 CDCR E-Mail

CDCR maintains an e-mail system to facilitate business communications and assist employees in performing their daily work activities.

The purpose of this Section is to establish guidelines for the administration, maintenance use of the CDCR e-mail system.

49020.20.1 Access to E-mail

CDCR staff may be provided an ID for access to e-mail, either on the CDCR Network or through an Internet Service Provider (ISP) if the CDCR Network is not available. All access to e-mail shall be protected by password, and all policies pertaining to the use and protection of passwords shall apply. No generic or group access to an ID shall be used. A "group mailbox" is acceptable as long as each individual in the group has their own ID and password.

If you require someone in addition to yourself to access or monitor your e-mail, establish a rule to forward/copy your mail to another's mailbox. Sharing a password for any reason is prohibited.

49020.20.2 Acceptable Use

The e-mail system is provided for official CDCR business. Using e-mail in an inappropriate manner may result in loss of e-mail privileges and/or disciplinary action.

Examples of appropriate use of the CDCR e-mail system include, but are not limited to, the following:

- Scheduling, coordinating, and documenting business meetings and/or assignments.
- Notifying CDCR personnel of changes in work policies and/or work procedures after the appropriate approval process has been completed (shall be followed up in writing).
- Transmitting and/or sharing nonconfidential work related material, including ducments, files, reference material, and links to Internet sites.
- Sending and receiving business related Internet mail.
- Notifying employees of CDCR sanctioned employee events including, but not limited to, the Medal of Honor ceremony, United California State Employees Campaigns, and similar approved activities.
- Scheduling appointments including personal appointments and lunch breaks on an electronic calendar.

49020.20.3 Unacceptable Use

Examples include, but are not limited to, the following:

- Using the system to discuss, distribute, or share confidential information.
- Reviewing, receiving, and/or intercepting the electronic communications of another employee without express, advance authorization by the employee or their management.
- Logging on with a user ID and password other than your own.
- Copying or routing notes, messages, documents, or memoranda to individuals who are not involved in the relevant work project or who otherwise have no business related interest in the subject matter of the note, message, document, or memorandum.
- Creating or sending notes or messages of a predominantly personal nature, or for personal gain.
- Except as otherwise provided in this Policy, reading e-mail of another employee without their knowledge and consent.
- Sending sports pool or other forms of gambling messages.
- Using e-mail for any unlawful or illegal endeavor.
- Soliciting or advertising for non-CDCR activities, including fundraising or items of a political nature.
- Allowing access to inmates or parolees, or sending messages on behalf of inmates or parolees.
- Transmitting profanity, obscenity, threatening language, gossip, or derogatory remarks.
- Distributing jokes, poems, chain-letters, or other nonbusiness related material.

49020.20.4 Privacy and Confidentiality

All e-mail is subject to unannounced inspections and should be treated like other shared filing systems. E-mail is not private and is subject to monitoring with or without notice.

49020.20.5 Personal Information

Employees shall not seek out or use personal information maintained by the CDCR for their own private interest or advantage. Personal information shall not be transmitted in e-mail or as attachments to e-mail. Confidential information shall not be transmitted via e-mail.

49020.20.6 Chain Letters, Jokes, and Other Non-CDCR E-Mail

Chain letters and e-mail containing religious, humorous, and political messages are forbidden. E-mail that contains promises, hoaxes, or threats shall not be distributed. Receipt of such e-mail should be reported to management. Forwarding of non-CDCR e-mail is forbidden. It is recognized that recipients cannot control in-coming mail. Use of CDCR e-mail for personal matters should be kept to a minimum. Personal e-mail is discouraged.

49020.20.7 Offensive Content

E-mail shall be free of offensive or unlawful material, including slanderous, discriminatory, sexual, pornographic, profane, or revolutionary content. This prohibition applies to e-mail attachments and to the content of Internet sites referenced or linked from e-mail. Displaying, printing, disseminating, or possession of such material may be reason for disciplinary action.

49020.20.8 Copyrighted Material

Use of the CDCR e-mail system to distribute copyright-protected material such as photographs, graphics, music, documents, etc., constitutes copyright violation, and may result in disciplinary action taken.

49020.20.9 Unsolicited E-Mail

Unsolicited e-mail may carry viruses. If the sender's identity and intent cannot be verified, such e-mail should be deleted unopened. Unsolicited e-mail from unknown senders should always be deleted unopened. Do not open attachments or Internet links accompanying such unsolicited e-mail.

49020.20.10 Use of Global Distribution Lists

Use of the global distribution list should be limited to departmental, State, or national emergencies, and information from executive levels or program areas that

affect all employees. Distribution of conformation not required by all employees should be limited to the affected work groups or physical locations.

49020.20.11 Incoming E-Mail

It is realized that recipients cannot control incoming e-mail. Use of the CDCR e-mail for personal matters is discouraged where and when possible.

49020.20.12 E-Mail Administration

EIS shall perform all administration functions including, but not limited to, establishment of server mailboxes, system-wide filters, and virus scanning functions. EIS shall determine the disk space required to ensure correct functionality of the e-mail system. Staff are strongly encouraged to move messages from their "server inbox" to their "personal folders" if retention is required. Retention of e-mail is governed by the CDCR document retention policies.

49020.20.13 E-Mail Virus Protection

EIS shall manage the virus protection program for all workstations, servers, and network devices. All workstations connected to the CDCR Network or are Internet accessible shall have the most current Virus Protection software, determined by the EIS. CDCR Network workstations shall be configured to automatic update of the virus protection software. Staff shall not disable or turn off this feature. Distribution of virus-laden e-mail may result in performance degradation of the CDCR network and the removal from the network of the workstation(s) from which the infected e-mail is sent.

49020.20.14 Additional E-Mail Usage Guidelines

Local operating procedures and guidelines may apply to e-mail content and handling. These local guidelines and procedures are in addition to this e-mail policy and may not be in conflict with or contradictory to this Policy.

49020.21 Electronic Document Management

The CDCR is committed to ensuring that all departmental electronic documents, including e-mail messages used by staff in the course of their employment, are retained efficiently and in compliance with the Records Management Act, GC, § 14740, et seq.

49020.21.1 Retention Schedules

In its statewide departmental Records Retention Schedule (RRS) (DOM, Chapter 1, Article 23, Records Retention), the CDCR sets the time periods after which State documents are destroyed. This Policy clarifies that the RRS extends to all electronic documents of the CDCR, including all e-mail messages and attachments to e-mail. These electronic documents include, but are not limited to, word processing files, spreadsheets, PowerPoint© presentations, and other computer displays.

Electronic documents stored both on local computers and network servers shall be deleted in accordance with the RRS, under the same time period that paper printouts of the documents would be disposed. Staff shall also, to the extent possible, delete all State electronic documents from stand-alone computer hard drives in accord with the RRS.

49020.21.2 E-Mail Retention

All opened e-mail shall be deleted from the CDCR statewide server after 30 days, and unopened e-mail shall be deleted after 90 days. Once it is deleted, e-mail cannot be retrieved from the server.

To preserve sent or received e-mail messages, staff may save those messages into personal folders within the e-mail program or elsewhere on their computer hard drive, or print them. Failure to move e-mail messages from the server will result in their automatic deletion from the server within the time frames noted above. Removal of e-mail from the server will not affect the contents of any personal folder. Staff is encouraged to save to a personal folder any e-mail messages that have an administrative, legal, or fiscal function related to their current work assignment. Those e-mail messages should then be deleted from the personal folders in accordance with the RRS.

49020.21.3 Reassignment of Workstations

The local computer coordinators shall erase all electronic documents from the hard drive of a computer once any staff member of the CDCR has ceased using that computer. All forms of electronic documents that the previous staff member created, received, or used shall be removed. As needed, the electronic documents may be transferred to another computer.

49020.22 Revisions

The Agency Information Security Officer, Office of Audits and Compliance, or designee shall be responsible for ensuring that the contents of this Article are kept current and accurate.

49020.23 References

The Constitution of the State of California, Article 1, Section 1.

The Information Practices Act of 1977, Civil Code § 1798.

The Federal Copyright Act of 1976.

The California Public Records Act.

PC, § 502.

SAM, §§ 1601-1699, 4820, 4841, 4841.3, 4842.1, 4989.7, 4990.1.

GC §§ 1222, 6250-6265, 14740-14770.

DOM §§ Chapter 1, Article 23, and Chapter 4, Articles 31, 40, 41, 45, 46, 48.

ARTICLE 46 — INFORMATION SYSTEMS RISK MANAGEMENT

Effective November 30, 1992

49030.1 Policy

Revised April 16, 1993

All ITS within the Department are subject to having a risk analysis prior to any approval or authorization for development or implementation. The result of this analysis, "The Risk Analysis and Risk Reduction Report," shall be submitted as part of the request for approval. This report is a part of the feasibility study for large systems, and stand-alone facilities within small systems. A multipurpose work station is exempt from this requirement unless there is a need for a modem or to store confidential or sensitive information.

49030.2 Purpose

The purpose of this policy is to identify and provide for the use of a generic systems approach as part of the Department's risk management program. This process shall assist users, systems designers, systems developers, and management in answering a number of basic questions, such as:

- What is the nature of the problem?
- What needs to be changed, modified, or accomplished?
- What alternatives are available to solve the problem?
- How, specifically, shall the problem be solved?
- How well does the new solution work?

49030.3 Responsibilities

The following is a description of the organizational responsibilities for administering this program.

The Director

The Director is responsible for establishing and maintaining a risk management program within the Department. It is the responsibility of the Director to assure that the Department's information assets are protected from the effects of damage, destruction, and unauthorized or accidental modification, access, or disclosure.

Specifically, the Director is responsible for ensuring the following:

- Enforcement of State-level risk management policies.
- Establishment and maintenance of internal policies and procedures that provide for the security of information technology facilities, software and equipment, and the integrity and security of the agency's automated information.
- Department compliance with reporting requirements related to risk management issues.
- Appointment of a qualified Information Security Officer (ISO).
- Participation of management during the planning, development, modification and implementation of risk management policies and procedures.

Information Security Officer

GC 1171 requires that the director of each agency designate an ISO. The ISO is responsible for overseeing agency policies and procedures designed to protect the Department's information assets. In accordance with State policy, the ISO shall be accountable to the CDC Director regarding these responsibilities.

To avoid conflicts of interest, the ISO shall not have direct responsibility for information processing, information access management functions, any departmental computer based systems or have a reporting relationship to an organization that has such responsibilities. The ISO shall not have any special allegiance or bias toward a particular program or organization.

The responsibilities of an ISO include overseeing the following:

- Implementation of necessary procedures to ensure the establishment and maintenance of a risk management program, including a risk analysis process.
- Establishment of procedures necessary to monitor and ensure compliance of established risk management policies and procedures.
- Coordination with internal auditors and QC personnel to define their role in automated ITS planning, development, implementation, operations, and modifications relative to risk management.
- Coordination with the data center's ISO or staff on matters related to the planning, development, implementation, modification, or risk management policies and procedures that affect the Department.
- Establishment of procedures to comply with control agency reporting requirements.
- Establishment of mechanisms to assure that Department staff (with particular emphasis on the owners, users and custodians of information) are educated and aware of their roles and responsibilities relative to risk management.
- Establishment of training programs for Department employees related to risk management.

Technical Management

Department technical management has the following responsibilities relative to CDC's risk management program:

- Ensuring that management, the ISO, assigned owners, and users/custodians are provided the necessary technical support services with which to define and select cost effective solutions to high risk problems identified through the risk analysis process.
- Ensuring the implementation of controls and procedures necessary to manage the risk identified through the risk analysis program.

Program Management

Department program managers have the following responsibilities in relation to CDC's risk management program:

- Establishing the procedures necessary to comply with risk management policy in relation to ownership, user and, if appropriate, custodian responsibilities.
- Ensuring the proper planning, development, and establishment of risk management processes and procedures for new computer-based systems and the files or data bases for which the program has ownership responsibility, and for new physical devices assigned to and located in the program area(s).

Program Personnel

Program personnel have the following risk management responsibilities:

- Implementing and monitoring data QA functions to ensure the integrity of data for which the program is assigned ownership responsibility.
- Complying with applicable federal, State, and Department risk management policies and procedures.
- Identifying information system vulnerabilities and informing program management and the ISO of those vulnerabilities.

Internal Auditors

Internal auditors have the following responsibilities in relation to the Department's risk management efforts:

- Examination of the Department's policies and procedures for compliance with State risk management policies.
- Examination of the Department's policies and procedures for compliance with control agency audit requirements.
- Examination of the effectiveness of the Department's policies and procedures, identification of inadequacies within the existing risk management program, identification of possible corrective actions, and informing management, the ISO, and the owners, custodians, and users of information of the findings.

QC

The designated responsible QC person/program has the following responsibilities in relation to the Department's risk management program:

- Review and evaluation of the risk management process used and its findings, to ensure the effectiveness of controls for automated ITS whether under design and development or operational, with particular emphasis on major systems.

Information Owners

The owners of information are responsible for classifying the information, filing security incident reports, securing and storing the signed security agreements, and identifying for the ISO the level of acceptable risk.

The owners of CDC information are identified in the system library document maintained by the MIS Support Unit.

Information users

It is the responsibility of all users to protect CDC resources, note variances from established procedures, and report such variances to the appropriate manager.

Information Custodians

The custodians of information are responsible for complying with applicable laws, policies, and procedures. It is also the responsibility of custodians to advise the owner and the ISO of any threats to the information, and notify the owner and the ISO of any violations of security policies, practices, or procedures.

49030.4 ITS--Risk Management Definitions

Audit Requirements

A section of the EDP audit reviews ITS documentation; each system not exempt from the audit requirements shall have an approved risk analysis report.

Critical Functions, System, and Resources

Elements vital to the organization's operation, and possibly to the continued, viable existence of the organization.

Current Risk

Current risks are evident and continuing, and are inherent to a business operation, location, or process.

Data Integrity

The state that exists when computerized data are the same as that in source documents and have not been exposed to accidental or malicious alteration or destruction.

Data Protection

Measures to safeguard data from occurrences that could lead to the modification, destruction, or disclosure of data.

Data Security

Protecting data from modification, destruction, or disclosure.

Potential Risk

Potential risk is outside normal and purposeful business operations, and results from some intentional or unintentional, indeterminate action.

Risk

Risk is a measure of the relative value attached to certain circumstances and conditions inherent in any business operation, or change to that operation. Risks are either current or potential.

Risk Analysis Content:

Technical Analysis

For each risk scenario, specify the threat and potential safeguards/controls identified. Each control should be discussed along with its intended purpose and the types of threats it is effective against. If no safeguards are found, then a statement to that effect shall be provided.

Operational Analysis

Each control identified above shall be analyzed and its impact on current operations should be discussed. All operational constraints that would make the safeguard difficult or impractical to implement or operate shall be discussed. Risks that shall be accepted due to the operational unacceptability of their safeguards shall be identified here.

Economic Analysis

For all controls that are technically and operationally feasible, discuss the cost benefit.

Risk Acceptance Summary

Lists all risks, acceptable or unacceptable. If acceptable, then indicate the basis for acceptance.

Controls Summary

Presents the controls to be used for eliminating or reducing the risks identified in the risk acceptance summary. Each control shall be described in terms of its loss reduction or effect, as well as the primary and secondary threat categories against which the control is effective.

Countermeasures

Any type of procedure (e.g., physical, procedural, hardware, software and personnel) used to counteract a threat to the system.

Risk Analysis Management Report:

Summary

A concise overview of the analysis. It shall begin with a statement describing the scope and objectives of the study, followed by the recommendations for risk acceptance and alternatives for reducing or eliminating the unacceptable risks.

Risk Scenario Summary

A summary of the essential data from the risk analysis.

Risk Management Process

Risk management is the work a manager does to identify the risk, assess its level, and create a plan for the acceptance, rejection, or control of the risk. This work is carried out by the application of a well-defined analytic process called "risk analysis," and culminates in a risk analysis report and risk reduction decision study.

Risk Analysis

Involves identifying the assets and resources that are at risk, as well as the threats to those assets and resources and the vulnerabilities in the risk environment that might allow the threats to materialize. Risk analysis also involves estimating the frequency with which the threats might occur, the safeguards currently in place, and the cost/impact that could be incurred if the threats to the risk environment were to materialize (this process correlates to the problem definition and analysis of the "current problem" steps in a generic systems approach).

Risk Reduction Analysis

Involves identifying the availability of potential safeguards, determining the operational and economic feasibility of potential safeguards, and developing a risk reduction decision study for presentation to management (this process correlates to the identification of alternatives, cost-benefit analysis, selection of best alternative, and conceptual system design phases of the generic systems approach).

Management Decision

Management decides which risks are acceptable. For those that are not currently acceptable, management decides which of the alternatives shall be implemented and approves the resources required to purchase, or design and develop, and then implement them (this process corresponds to the management decision phase of the generic systems approach).

Development of Risk Reduction Plans

Outlines the tasks to be performed to implement the safeguards selected by management. Tasks include identification of the specific safeguards, assignment of responsibility for design, development or purchase, and implementation of the safeguards. Plans shall also include a timetable of the milestones leading to implementation (this process corresponds to the detailed design and development/testing phases of the generic systems approach).

Implementation and Maintenance of Safeguards

Involves the installation, operation and maintenance of new or modified safeguards. Implementation shall involve personnel training and coordinating any changes in operations with affected personnel.

Vulnerability

Susceptibility of a system to a specific threat, attack or harmful event, or the opportunity available for a threat agent to mount such an attack.

Vulnerability Assessment

A review of a system or program to determine its susceptibility to loss or unauthorized use.

49030.5 ITS - Risk Management New System Requests

All requests for approval for new systems development shall indicate if the system is a critical application.

49030.6 ITS - Risk Management Critical Applications

All critical applications shall require a risk analysis. See DOM 49040, Procedures.

49030.7 ITS - Risk Management Other Systems

Revised April 16, 1993

A risk analysis shall be submitted to the Information Security Unit (ISU) for all systems that are non-critical applications but use one or more of the following:

- Telecommunications.
- Programs created or maintained by inmates.
- Inmates as keyboard operators.

These applications require a risk analysis approved by ISU prior to implementation.

The MIS Committee may direct that a risk analysis be carried out for any new system when deemed necessary.

49030.8 Risk Management Exemption for Inmate Use

Requests to ISU for an exemption from information security policy, as it pertains to inmates and computers shall be accompanied by a risk analysis. An exemption shall only be granted by the MIS Committee based upon the risk analysis and a recommendation by ISO.

49030.9 Revisions

Revised April 16, 1993

The Assistant Director, OOC, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

49030.10 References

GC § 1171.

DOM § 49040.

ARTICLE 47 — DISASTER RECOVERY PLANNING

Effective November 30, 1992

49040.1 Policy

It is the policy of the Department that each element of the Department utilizing information technology shall establish disaster recovery planning processes for identifying, assessing, and responding to the risks associated with its information assets. See the DOM 49010 for additional details.

49040.2 Purpose

The purpose of disaster recovery planning is to ensure continuity in computer operations for the support of critical applications, provide the greatest possible benefit from remaining limited resources, and achieve a systematic and orderly migration toward the resumption of all automation activities within the affected segment of the Department.

49040.3 Classification of Computers According to Type

The information assets of the Department are distributed over many geographically separated entities. However, any usage of computer resources in CDC will fall within one of four different types. The primary factors associated with each type represent the complexity and scope of operational use of the computer or system involved. In the context of this policy, "system" means a computer program and the computer resources necessary to achieve the objective of the program. It is possible for similar computers to be classified differently depending upon the program being used. This is especially true in the inmate education area. DOM 47000 contains information on each of the critical systems utilized by the Department.

Type 1

Most of the large, Departmentwide computer systems are comprised of a computer at a central site, and a telecommunication network (phone lines) with terminals, printer, modems, and controllers located at a local site. Examples of this type of configuration include the OBIS, the Inmate Trust System, and the Personnel and Leave Accounting System.

Each of these systems would be affected by any disaster occurring within the data center or any disaster that would disrupt part or all of the communication lines. While the operational recovery of these systems is the data center's responsibility, each of the user sites shall have contingency plans ready to enable actions that minimize disruptions to business activities.

Type 2

The computer-based system is approved for departmental use and is to be implemented at all appropriate sites. This type of system can be found at many sites. These systems are not connected electronically. Each site uses the same programs to support the same work. Examples of Type 2 systems are the Critical Case Factor System and the microcomputer-based Inmate Appeals System: both of these are examples of stand-alone departmental ITS.

Type 3

This type of computer system is normally found at only one site. Type 3 systems are created because the multipurpose work station is available and there is an identified need.

Type 4

Type 4 systems are found only in the academic or vocational education areas. These systems are intended to be used strictly for the education of inmates.

49040.4 Responsibilities

The CDC approach to risk management requires that active support and ongoing participation be obtained from individuals representing multiple disciplines and all management levels. This includes the support of executive, program, and technical management, as well as owners, custodians, and users of the information.

Director

It is the responsibility of the Director to assure that the Department's information assets are protected from the effects of damage, destruction, and unauthorized or accidental modification, access, or disclosure. Specifically, the Director is responsible for ensuring the following:

- Enforcement of State-level operational recovery policies.
- Establishment and maintenance of internal policies and procedures that provide for the security of information technology facilities, software, and equipment, and the integrity and security of the Department's automated information.
- Department compliance with reporting requirements related to operational recovery.
- Preparation and maintenance of the Department's operational recovery plan, and the continuation of vital information support services in case of a disaster.
- Participation of management during the planning, development, modification, and implementation of operational recovery policies and procedures.

Information Security Officer

GC 1171 requires that the director of each State agency designate an Information Security Officer (ISO). The ISO is responsible for overseeing agency policies and procedures designed to protect the Department's information assets. In accordance with State policy, the ISO shall be responsible to the CDC Director for such responsibilities.

Additionally, to avoid conflicts of interest, the ISO shall not have direct responsibility for information processing, information access management functions, or any departmental computer based systems, or have a reporting relationship to an organization that has such responsibilities. The ISO shall not have any special allegiance or bias toward a particular program or organization.

The responsibilities of an ISO include overseeing the following:

- Development and maintenance of an operational recovery plan to protect the Department against the potential effects of a disaster.
- Establishment of procedures to comply with control agency reporting requirements relating to operational recovery.

Technical Management

Department technical management has the following responsibility relative to the Department's operational recovery program:

- Ensuring the implementation and maintenance of an operational recovery plan in cooperation with Department management, the ISO, and the assigned owners, users, and custodians of information.

Program Management

Department program managers have the following responsibilities in relation to the CDC security program:

- Establishing procedures necessary to comply with operational recovery policy pertaining to ownership, user, and, if appropriate, custodian responsibilities.
- Ensuring that operational recovery plans are in place for hardware, software, and files or data bases for which the program is assigned ownership responsibility.
- Ensuring that custodians of program information are provided the appropriate direction to implement the operational recovery plans that have been defined.
- Ensuring that procedures are established to comply with departmental operational recovery reporting requirements.

Internal Auditors

Internal auditors have the following responsibilities in relation to the Department's operational recovery planning efforts:

- Examination of the Department's policies and procedures for compliance with State policies.
- Examination of the Department's policies and procedures for compliance with control agency audit requirements.
- Examination of the effectiveness of the Department's policies and procedures; identification of inadequacies within the existing operational recovery programs, and identification of possible corrective actions.
- Provision of applicable findings to management, the ISO, and the owners, custodians, and users of information.

QC

The designated responsible QC person/program has the following responsibilities in relation to the Department's operational recovery program:

- Review and evaluation of the effectiveness of operational recovery plans for automated ITS, whether under development or operational, and with particular emphasis on major systems.

Information Owners

The owners of information are responsible for classifying the information, defining precautions for controlling access, disposing of the information, authorizing/denying access to the information, filing security incident reports, securing the signed security agreements and storing them for reference, and identifying (for the ISO) the level of acceptable risk.

The owners of CDC information are identified in the system library document maintained by the MIS-SU.

Information Users

It is the responsibility of all users to protect CDC resources, to note variances from established procedures, and to report such variances to the appropriate manager.

Information Custodians

The custodians of information are responsible for complying with applicable laws and policies, complying with policies and procedures established by the owner and the ISO, advising the owner and the ISO of any threats to the information, and notifying the owners and the ISO of any violations of security policies, practices, or procedures.

49040.5 Definitions

Application Disaster Recovery Plan

A plan devised to process an application after it has been disrupted for some period of time.

Back-up Procedures

Methods used to recover computer programs and files after a disaster or system failure.

Contingency Planning

The procedure of developing a back-up plan to restore business and data center operations in the event of a disaster or interruption. Also called “disaster recovery planning” or “business resumption planning.”

Contingency Program

The everyday work activities and procedures (e.g., backing-up critical data files) that fulfill the requirements of recoverability.

Disaster

A human or natural occurrence causing destruction and distress, after which a business is deemed unable to function.

Disaster Recovery Operation

The act of recovering from the effects of disruption to a computer facility, and the pre-planned restoration of facility capabilities.

Disaster Recovery Plan

The preplanned steps that make possible the recovery of a business computer facility or the applications processed therein. Also called a "contingency plan" or "business resumption plan."

Emergency Response

The immediate action taken to protect hardware and sensitive magnetic media in the event of natural disasters, fire, power failures, equipment breakdown, theft, vandalism, or tampering.

49040.6 Disaster Recovery Planning-Critical Systems

Revised April 16, 1993

Department Operational Recovery Plan

The Department operational recovery plan shall cover a minimum of four topic areas:

- Summary of the strategy for managing disaster situations.
- Distinct management and staff assignment of responsibilities immediately following a disaster and continuing through the period of normal operations re-establishment.
- Priorities for the recovery of critical applications.
- Operational procedures documented in systematic fashion that shall allow recovery to be achieved in a timely and orderly way.

Type 1 and Type 2 Operational Recovery Plans

All Type 1 and Type 2 systems shall require an operational recovery plan that answers the following questions:

- Identification and evaluation of alternative recovery strategies.
- Selection of the alternative that best responds to the organization's requirements for disaster recovery.
- Assessment of the resource requirements (space, equipment, communications, data, software, personnel, and time) required for operational recovery of the critical application.

49040.7 ITS Disaster Recovery Coordinator (ISDRC)

The ITS Disaster Recovery Coordinator (ISDRC) for CDC is the computer operations section manager from ISD.

49040.7.1 Responsibilities of the ISDRC

Revised April 16, 1993

The ISDRC is responsible for maintaining a Department operational recovery plan that identifies computer applications deemed critical to the Department's operations, the information assets that are necessary for those applications, and the Department's plans for resuming operations following a disaster affecting those applications. The ISDRC shall coordinate the preparation of the operational recovery plan with the disaster recovery coordinator of the Institutions Division and with the CDC Data Center. The ISDRC is responsible for ensuring that periodic testing of the Department operational recovery plan is carried out.

49040.8 Submitting the Disaster Recovery Operational Recovery Plan

The CDC Disaster Recovery Coordinator shall file an informational copy of the Department operational recovery plan with the Office of Information Technology, DOF, no later than January31 of each year. A copy of this plan shall be sent to the Teale Data Center.

49040.9 Approval of New Critical Department ITS

Revised April 16, 1993

Each request for approval to proceed with the development of a critical Department information system shall address the issue of the operational recovery of the system to be developed. All resource requirements associated with the operational recovery methods shall be identified as part of the critical ITS' cost.

Prior to the implementation of any critical system, project management shall submit to ISD a copy of the critical system's operational recovery plan for inclusion in the annual submittal to the control agency.

49040.10 Revisions

Revised April 16, 1993

The Chief, ISD, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

49040.11 References

Revised April 16, 1993

GC § 1171.

DOM § 47000.

DOM § 49010.

ARTICLE 48 — ELECTRONIC DATA PROCESSING AUDITING

Revised April 16, 1993

49050.1 Policy

It is the policy of the Department to conduct EDP audit activities as required in the SAM and as is necessary to ensure maximum efficiency and productivity resulting from use of the Department's automated information resources. Such activities shall include a biennial EDP audit, as specified in this section, with a copy of each such audit provided to the Financial and Performance Audit Unit (FPA) of the DOF.

The biennial EDP audit report shall be structured to meet the requirements of SAM 20013, Review and Reporting on Computer-Based Systems, as well as the FPA audit guidelines, which provide evaluation criteria to determine the Department's compliance with the policies contained in SAM 4840 through 4845, and 4989.7. In addition, the departmental EDP audit process shall determine compliance with the policies contained in the DOM 49000, Information Security, Risk Management and Operational Recovery.

49050.2 Purpose

The purpose of this policy is to establish and maintain a standard of due care to prevent misuse or loss of Department information assets.

49050.3 Responsibility

PFAB shall be responsible for the biannual EDP audit.

49050.4 Types of EDP Auditing

There are four main types of audits:

Financial Audit

Determines the reliability and integrity of financial statements. Audit information is used generally by individuals other than management.

Compliance Audit

Ascertains compliance with specific policies, procedures, laws, regulations, or contracts affecting operations or reports.

Operational Audit

Usually includes a review of internal controls, compliance, integrity of operating information, use of resources, and achievement of goals.

EDP Audit

Combines both the compliance audit (specific EDP policies, procedures, etc.) and the operational audit; probes the integrity and reliability of computer processing and its contribution to operating information. EDP auditing can become very complex, since it is desirable to examine the controls within systems that are used to protect the integrity of data.

49050.5 Revisions

The Assistant Director, OOC, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

49050.6 References

SAM §§ 4840 - 4845, 4989.7, and 20013.

DOM § 49000.

ARTICLE 49 — SPECIAL SECURITY CONSIDERATIONS

Effective November 30, 1992

49060.1 Policy

It is the policy of the Department that the secure protection of EDP capabilities and information requires special resources and considerations when the information involved is sensitive or confidential in nature. In such instances, augmented security measures shall be implemented

49060.2 Purpose

The purpose of this section is to clarify that, in addition to other EDP security policies and procedures contained in this manual, all CDC employees shall, where applicable, adhere to the security requirements of this section. This section outlines the responsibilities of the Department, Security Coordinator, and Security Monitors pertaining to certain personnel and payroll information.

49060.3 Responsibilities

Department

CDC shall appoint a departmental Security Coordinator from within the personnel/payroll office with responsibilities sanctioned by the SCO. A Security Monitor shall be appointed at each facility. The Security Coordinator and Security Monitors shall have access to the SCO system and database.

Security Coordinator

The Security Coordinator shall perform the following duties:

- Act as a liaison with the SCO decentralized Security Coordinator.
- Act as the security resource for all departmental personnel/payroll office employees and Security Monitors in facility personnel offices.
- Authorize, approve, and maintain security clearance requests (PSD Form 125A) on behalf of the SCO to determine whether an individual shall be granted access to the SCO database.
- Monitor all physical security elements and barriers to maintain the SCO's security requirements.
- Report all security infractions and violations to the SCO decentralized Security Coordinator and the CDC Information Security Officer (ISO).

- Coordinate activities associated with the movement, alteration, addition, or removal of approved equipment with the local information security coordinator and ISD.
- Monitor access to restricted areas within personnel units, and approve/disapprove the clearance of individuals requesting access to the decentralized personnel site.
- Maintain all records regarding individuals approved for access to the system, including all present and past Security Monitors. This information shall be provided to the Chief, SCO Information Security Office, and the SCO Division of Audits.

Security Monitors

Security Monitors are located in those facility personnel offices having access to the SCO database. Each Security Monitor shall adhere to the Department information security policy and, in addition, shall:

- Monitor all physical security elements and barriers to maintain SCO security requirements.
- Report all security infractions and violations to the Security Coordinator.
- Notify the Security Coordinator of all activities associated with the movement, alteration, addition, or removal of approved equipment.
- Monitor access to restricted areas, and approve/disapprove the clearance of authorized individuals requesting access to the decentralized site.

49060.4 Special Site Security Considerations

The sites of SCO computer equipment shall be kept secure (by means of locking devices, guards, badges or barriers) from unauthorized physical or visual access. The site shall be located in an area restricted from the public and unauthorized employees. Entry shall be monitored during work hours, and restricted areas shall be locked when unattended. Keys shall be distributed on a limited and controlled basis to authorized employees only.

Layout plans for equipment shall include the following:

Floor Plan

- The site layout shall include an analysis of employee work areas, the manner in which employees shall enter and exit the office, the location of SCO equipment, and the location and type of all locking devices and barriers.

Doors

- Doors shall be solid, locking, full or Dutch-style doors that are accessible only with the correct key or electronic key/badge. Doors shall remain closed and locked at all times.

Windows

- Interior windows shall be frosted or covered completely to eliminate visual access to the terminal screens. Exterior windows on a ground floor shall be frosted, covered, and secured if easily opened.

Locks

- Locks shall be installed on all interior and exterior doors allowing access to the secured area. Acceptable locks include, but are not limited to, the following:
  - Key-controlled locks.
  - Code-controlled locks.
  - Electronic locks.
  - Double-bolting locks Dutch doors.

Counters

- If a counter exists in the secured area, access into the work area shall be controlled and monitored. Records of approved access shall be maintained by the Security Monitor.

Changes To Site

Any changes to an approved, decentralized site require prior, written SCO approval. Requests for site changes shall include a diagram of the proposed site including the proposed location of equipment. Unauthorized movement of decentralized equipment may result in the loss of system access.

49060.5 Special Equipment Security Considerations

To ensure the security of SCO equipment and information, personnel employees shall adhere to the following equipment security guidelines:

- Equipment shall be located in restricted areas that are monitored during working hours and locked during any unattended periods.
- Only authorized employees shall have access to terminals, printers, control units and modems.
- System access shall be completely signed off when not in use.
- Terminals shall be locked, keys removed, and screen intensity turned completely down when the terminals are unattended.

The following shall be stored in a vault or locked cabinet when not in use:

- Keys to terminals.
- Manuals for system software and hardware.
- Other instructional and operational manuals.

No equipment shall be attached to any authorized configuration of decentralized equipment, except for testing and installation tools used by the vendor or telephone company.

Deviations from the requirements listed above shall have prior written approval from the SCO Security Coordinator.

Equipment Changes

The following types of changes to the SCO decentralized system require prior, written approval from the Security Coordinator:

- Changes of any kind to the location of decentralized equipment.
- Switching of terminals from one control unit to another.
- Any additions or removals of decentralized equipment.

49060.6 Special Data Security Considerations

Personnel employees shall consider all information residing in the SCO database as sensitive and confidential, and shall protect information from unauthorized access.

Hardcopy

Employees shall consider all data hardcopy (including printouts) gained from the SCO system as confidential, and shall handle and destroy hardcopy accordingly. The various user manuals provided by the SCO contain confidential access instructions and shall be stored in a vault or locked cabinet when not in use.

Authorized Personnel

Access to information provided through the SCO system is restricted to authorized personnel. Only the following persons shall be considered authorized personnel:

A state employee or bona fide representative of the SCO who:

- Demonstrates either a need for or a legal right to the information;
- Receives formal authorization from the security coordinator; and,
- Accepts legal responsibility for preserving the security of the information.

Persons who require access to the SCO system shall demonstrate the need for such access by defining their specific, relevant duties. Any change in these duties requires a reevaluation of the need for access.

Access shall be revoked if the need for access no longer exists.

User Identification

Each person authorized to access the SCO system shall be provided with a unique user identification (ID). Requests for a new user ID or an ID revocation shall be directed to the Security Coordinator.

CDC employees are required to read SCO's Security Guidelines and sign the PSD Form 108, Statement of Understanding, prior to receiving access to SCO. New IDs and ID revocations are recorded on the PSD Form 125A.

Passwords

Access to the SCO system is restricted through the use of passwords. Use of any user ID also requires the associated password, known only to its owner. Passwords shall be changed monthly.

To protect system security, the ID owner shall <u>not</u>:

- Reveal the password to anyone.
- Write the password on any media.
- Walk away from an active terminal session; users shall log off the system prior to leaving.
- Log on in order to provide access or allow use by any unauthorized person.
- Use an obvious password, such as the owner's nickname, or any other easily identifiable password.

If a password does not operate correctly and the ID owner is sure that the correct password has been used, the owner shall notify the Security Coordinator immediately.

An ID owner who has forgotten the password shall contact the SCO Information Security Office.

Anyone who suspects that a password has been compromised shall notify the Security Coordinator immediately.

49060.7 Revisions

Revised April 16, 1993

The Chief, ISD, or designee shall be responsible for ensuring that the contents of this section are kept current and accurate.

49060.8 References

Revised April 16, 1993

SAM §§ 4840 - 4845, 4989.7, and 20013.